salesforce

# Impostazione e gestione dell'organizzazione Salesforce

Guida dell'utente, Winter '16

@salesforcedocs

# SOMMARIO

# Impostazione e gestione dell'organizzazione Salesforce

## Un benvenuto agli amministratori di Salesforce

Un amministratore di Salesforce (un utente assegnato al profilo Amministratore) è responsabile dell'impostazione dell'organizzazione online, ovvero dell'inserimento degli utenti e della configurazione del sistema in funzione delle esigenze.

Questa guida contiene le informazioni necessarie per impostare e gestire un'organizzazione Salesforce.

Ci auguriamo che questa guida fornisca tutte le informazioni necessarie per mettere l'organizzazione in condizioni di utilizzare Salesforce. Se fossero necessari ulteriori chiarimenti, contattare il team di assistenza in Salesforce.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: tutte le versioni

## Versioni di prova di Salesforce

### Panoramica sulla versione di prova

Il periodo di prova consente di valutare Salesforce prima di abbonarsi. La versione di prova comprende:

- Dati di esempio. È possibile eliminare i dati di esempio.
- Privilegi dell'amministratore. La persona che si è abbonata diventa automaticamente l'amministratore. È possibile aggiungere un altro amministratore quando si aggiungono altri utenti.
- Un'ampia gamma di funzioni di Salesforce.
- La possibilità di abbonarsi a Salesforce.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

Nota: Le funzioni incluse nella versione di prova potrebbero non essere disponibili nella versione (Edition) che si sceglierà di acquistare.

Se si impostano più utenti per la versione di prova e in seguito si decide di passare alla versione Personal Edition, tutti gli utenti ad eccezione dell'amministratore originario del sistema verranno disattivati.

# Avvio di una nuova prova

Al momento dell'iscrizione a Salesforce, è possibile scegliere un modello specifico per il proprio settore con dati di esempio. Nel corso del periodo di prova è possibile avviare una nuova prova con un modello vuoto. Per avviare una nuova prova è necessario abbandonare quella corrente, compresi tutti i dati e le personalizzazioni.

È possibile avviare una nuova prova se si dispone di quanto segue:

- Meno di 1000 righe di dati
- Nessuna licenza utente supplementare aggiunta da Salesforce
- Nessuna funzione supplementare abilitata da Salesforce

Per avviare una nuova prova:

1. Da Imposta, immettere *Inizia una nuova prova* nella casella `Ricerca veloce`, quindi selezionare **Inizia una nuova prova**. Il collegamento è disponibile solo durante il periodo di prova.
2. Selezionare la lingua e le preferenze per il modello.
3. Immettere i dati richiesti e confermare l'intenzione di abbandonare l'organizzazione di prova corrente e tutti i relativi dati, inclusi i dati di esempio immessi in precedenza.
4. Selezionare la casella per confermare che tutti i dati di prova correnti andranno perduti.
5. Fare clic su **Invia**.
6. Quando viene visualizzata la pagina di conferma, fare clic su **Invia**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

AUTORIZZAZIONI UTENTE

**Autorizzazioni utente richieste**

Per avviare una nuova prova:
- "Modifica tutti i dati"

Nota: quando si decide di avviare una nuova prova, si abbandona l'organizzazione di prova corrente, compresi tutti i dati e le personalizzazioni. Non sarà più possibile accedere alla prova o ai dati e solo i nomi utente saranno conservati.

# Conversione di una versione di prova mediante Checkout

Gli utenti con un account Checkout possono convertire una versione di prova di Salesforce in un abbonamento a una versione. Se la propria organizzazione non dispone di un accesso self-service a Checkout, inviare una richiesta al rappresentante Salesforce.

Per convertire una versione di prova in abbonamento mediante Checkout è necessario creare un preventivo.

Nota: in qualsiasi fase del processo di creazione del preventivo è possibile fare clic su **Richiesta di assistenza commerciale** per contattare un addetto alle vendite Salesforce.

Per convertire una versione di prova in abbonamento:

1. Per creare un preventivo, fare clic su **Abbonati ora** o selezionare Checkout dall'elenco a discesa delle applicazioni Force.com. Tenere presente che la versione (Edition) e i prodotti utilizzati nell'organizzazione di prova sono preselezionati in Checkout.

   Importante: se durante la creazione dell preventivo si chiude la finestra, tutte le modifiche andranno perse. Se si sta creando un nuovo preventivo, andrà persa l'intero preventivo. Fare clic su **Salva per uso successivo** in qualsiasi pagina se si desidera salvare le modifiche e continuare in un secondo tempo.

2. Se si è un nuovo utente o si sta creando o modificando un preventivo da una versione di prova, immettere e confermare le informazioni nella scheda Informazioni abbonamento.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Personal Edition**, **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

3. In caso di creazione o modifica di un preventivo da una versione di prova più estesa, immettere e confermare le informazioni nella pagina Prodotti, controllare i dati di fatturazione e fare clic su **Passa a Revisione ordine**.
4. Per creare un preventivo da un'altra versione, fare clic su **Versioni e prezzi**. Immettere e confermare i dati relativi all'abbonamento, al prodotto e alla fatturazione, quindi fare clic su **Passa a Revisione ordine**. La pagina Revisione ordine mostra i dati inseriti, oltre ai prezzi completi di tutti i prodotti presenti nel preventivo.

   Nota: Se si converte un'organizzazione in prova in una versione meno importante, ad esempio passando da una versione di prova Professional Edition a un abbonamento alla versione Group Edition, alcune funzioni e dati della versione di prova vengono eliminati. Per accettare l'eliminazione, selezionare la casella di controllo `Conferma`. Fare clic su **Rivedi** per visualizzare un elenco delle funzioni non supportate nella versione scelta. Se si desidera eseguire il backup di tutti i dati prima della conversione, accedere all'organizzazione Salesforce e da Imposta, immettere *Esportazione dati* nella casella `Ricerca veloce`, quindi selezionare **Esportazione dati**.

5. Verificare l'acquisto e fare clic su **Emetti ordine**.

Se un utente in prova crea un preventivo ma non emette l'ordine, il preventivo viene salvato in Checkout. Una volta completato un preventivo ed emesso un ordine per l'abbonamento a una versione, gli eventuali altri preventivi aperti relativi ad altre versioni vengono chiusi.

VEDERE ANCHE:

Guida dell'utente di Checkout

# Eliminazione dei dati della versione di prova

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

AUTORIZZAZIONI UTENTE

Per eliminare dati del periodo di prova:
- "Modifica tutti i dati"

Quando si sottoscrive l'abbonamento a Salesforce, il sistema dell'organizzazione viene compilato con dati di esempio. Durante il periodo di prova, gli amministratori possono eliminare tutti i dati di esempio e tutti i dati dell'organizzazione utilizzando il link Elimina tutti i dati.

Nota: Il link Elimina tutti i dati è visibile solo quando sono soddisfatte tutte le condizioni seguenti.
- L'utente dispone dell'autorizzazione "Modifica tutti i dati".
- L'organizzazione è in stato di prova.
- L'organizzazione non ha abilitato alcun portale.
- L'utente non è un Amministratore partner, operante per conto di un altro utente.

Per eliminare tutti i dati esistenti nella versione di prova:

1. Da Imposta, immettere *Elimina tutti i dati* nella casella `Ricerca veloce`, quindi selezionare **Elimina tutti i dati**.
2. Immettere i dati richiesti e confermare di essere al corrente che tutti i dati dell'organizzazione verranno eliminati, inclusi i dati di esempio immessi in precedenza. Le impostazioni utente e amministratore non subiranno alcuna modifica.
3. Fare clic su **Invia**.

Al termine del periodo di prova è possibile eliminare i dati di esempio manualmente o con la funzione di Eliminazione globale.

# Impostazione dell'organizzazione

## Come trovare informazioni sulla società

Trovare le informazioni fornite quando la società si è registrata con Salesforce nella pagina Informazioni sulla società in Imposta.

Dalla pagina Informazioni sulla società è possibile:

- Modificare le impostazioni sulla società.
- Visualizzare le licenze utente, le licenze funzioni, le licenze insiemi di autorizzazioni e i diritti basati sull'utilizzo a cui ha accesso l'organizzazione.
- Aggiungere o rimuovere licenze.
- (Solo organizzazioni Sandbox) Abbinare le licenze predisposte nell'organizzazione di produzione all'organizzazione Sandbox. Il processo di abbinamento aggiorna l'organizzazione Sandbox con le licenze della produzione ed elimina eventuali licenze che sono presenti nel Sandbox e non nella produzione.

VEDERE ANCHE:

Campi Informazioni sulla società

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

AUTORIZZAZIONI UTENTE

Per visualizzare le informazioni sulla società:
- "Visualizza impostazione e configurazione"

Per modificare le informazioni sulla società:
- "Modifica tutti i dati"

## Campi Informazioni sulla società

La pagina Informazioni sulla società contiene i seguenti campi (elencati in ordine alfabetico), ivi comprese le licenze utente e funzioni acquistate per l'organizzazione.

| Campo | Descrizione |
|---|---|
| `Indirizzo` | Indirizzo postale dell'organizzazione. Questo campo consente fino a 255 caratteri. |
| `Newsletter amministratore` | Consente agli amministratori dell'organizzazione di decidere se desiderano ricevere messaggi email promozionali destinati agli amministratori da Salesforce. |
| `Richieste API, ultime 24 ore` | Numero totale di richieste API effettuate dall'organizzazione nelle ultime 24 ore. Il numero massimo di richieste dipende dalla versione (Edition) utilizzata. |
| `Città` | Città in cui ha sede l'organizzazione. Questo campo consente fino a 40 caratteri. |
| `Valuta aziendale` | Valuta in cui la sede centrale dell'organizzazione compila le dichiarazioni dei redditi. Funge da base per tutti i tassi di conversione delle valute. |

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

I campi disponibili variano secondo la versione (Edition) di Salesforce utilizzata.

| Campo | Descrizione |
| --- | --- |
| | Solo per le organizzazioni che utilizzano più valute. |
| `Paese` | Porzione dell'indirizzo dell'utente che indica la nazione. La voce viene selezionata da un elenco di valori standard o immessa come testo. Se il campo è un campo di testo, sono ammessi fino a 80 caratteri. |
| `Creato da` | Utente che ha iscritto l'organizzazione, comprese la data e l'ora di creazione. (Sola lettura) |
| `Impostazioni internazionali valuta` | Paese o area geografica in cui ha sede l'organizzazione. Questa impostazione influisce sul formato degli importi in valuta. Solo per le organizzazioni con una sola valuta. |
| `Lingua predefinita` | Lingua predefinita selezionata per i nuovi utenti dell'organizzazione. Questa impostazione determina la lingua utilizzata per l'interfaccia utente e la guida in linea. In tutte le versioni tranne la Personal Edition e Database.com, i singoli utenti possono impostare separatamente la lingua per il proprio accesso, sostituendo l'impostazione dell'organizzazione. Nella versione Group Edition, questo campo è denominato `Lingua di visualizzazione`.<br>Questa impostazione determina inoltre la lingua in cui vengono memorizzate tutte le personalizzazioni (campi personalizzati, schede e opzioni dell'interfaccia utente). Nel caso delle personalizzazioni, le lingue definite dai singoli utenti non sostituiscono questa impostazione.<br>Se si modificano o si clonano i criteri di filtro già esistenti, assicurarsi che l'impostazione corrisponda alla lingua predefinita configurata durante l'impostazione del criterio di filtro originale. In caso contrario, i criteri di filtro potrebbero non essere valutati come previsto. |
| `Impostazioni internazionali predefinite` | Paese o area geografica predefinita selezionata per i nuovi utenti dell'organizzazione. Questa impostazione determina il formato delle date, degli orari e dei nomi in Salesforce. Nelle organizzazioni che utilizzano le versioni Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition e Developer Edition, i singoli utenti possono definire le proprie impostazioni internazionali, che sostituiscono le impostazioni aziendali. Nella versione Group Edition, questo campo è denominato `Impostazioni internazionali`. |
| `Fuso orario predefinito` | Fuso orario principale in cui ha sede l'organizzazione. L'impostazione del `Fuso orario` dei singoli utenti sostituisce l'impostazione del `Fuso orario predefinito` dell'organizzazione. |

| Campo | Descrizione |
| --- | --- |
| Divisione | Gruppo o divisione che utilizza il servizio, ad esempio Gruppo vendite PC. Questo campo consente fino a 40 caratteri. |
| Fax | Numero di fax. Questo campo consente fino a 40 caratteri. |
| Inizio anno fiscale | In caso di utilizzo di un anno fiscale standard, il mese e l'anno di inizio dell'anno fiscale dell'organizzazione. In caso di utilizzo di un anno fiscale personalizzato, il valore sarà "Anno fiscale personalizzato". |
| Nascondi avvisi sull'inattività del sistema | Selezionare questa casella di controllo per evitare che gli utenti visualizzino preavvisi relativi a periodi di inattività pianificati del sistema quando accedono a Salesforce. |
| Nascondi avvisi sulla manutenzione del sistema | Selezionare questa casella di controllo per evitare che gli utenti visualizzino preavvisi relativi alla manutenzione pianificata del sistema quando accedono a Salesforce. |
| Modificato da | Utente che ha modificato per ultimo le informazioni relative alla società, incluse la data e l'ora della modifica. (Sola lettura) |
| Newsletter | Consente agli utenti dell'organizzazione di decidere se desiderano ricevere messaggi email promozionali destinati agli utenti da Salesforce. |
| Nome organizzazione | Nome dell'organizzazione. Questo campo consente fino a 80 caratteri. |
| Telefono | Numero di telefono principale dell'organizzazione. Questo campo consente fino a 40 caratteri. |
| Referente principale | Persona che funge da referente principale o amministratore nell'organizzazione. È possibile digitare un nome o selezionarne uno da un elenco di utenti definiti in precedenza. Questo campo consente fino a 80 caratteri. |
| Accessi limitati, mese corrente | Numero di utenti con accesso limitato che si sono autenticati nel mese corrente.<br>Questo valore viene azzerato all'inizio di ogni mese. Il numero massimo di utenti con accesso limitato per l'organizzazione è indicato fra parentesi. |
| Licenze Salesforce | Numero di account utente Salesforce che è possibile definire per l'accesso al servizio. Questo è il numero delle licenze utente Salesforce fatturate all'organizzazione qualora siano a pagamento. |
| ID organizzazione Salesforce | Codice che identifica in modo univoco l'organizzazione in Salesforce. |
| Stato/Provincia | Porzione dell'indirizzo dell'utente che indica lo stato o la provincia. La voce viene selezionata da un elenco di valori standard o immessa |

| Campo | Descrizione |
|---|---|
| | come testo. Se il campo è un campo di testo, sono ammessi fino a 80 caratteri. |
| `Eventi Streaming API, durata 24 ore` | Il numero totale di eventi Streaming API utilizzati dall'organizzazione nelle ultime 24 ore. Il numero massimo di eventi dipende dalla versione (Edition) utilizzata. |
| `CAP` | Codice postale dell'organizzazione. Questo campo consente fino a 20 caratteri. |
| `Spazio dati utilizzato` | Quantità di memoria dati utilizzata; il valore è espresso come misura (ad esempio 500 MB) e come percentuale della memoria dati totale disponibile (ad esempio il 10%). |
| `Spazio file utilizzato` | Quantità di memoria file utilizzata; il valore è espresso come misura (ad esempio 500 MB) e come percentuale della memoria file totale disponibile (ad esempio il 10%). |

VEDERE ANCHE:

Come trovare informazioni sulla società

# Domini obbligatori

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: tutte le versioni.

Per mettere a disposizione i contenuti, Salesforce utilizza i domini seguenti.

- *.content.force.com
- *.force.com
- *.salesforce.com
- *.staticforce.com

Se i domini vengono inseriti in una whitelist, aggiungerli all'elenco di quelli consentiti. Se sono stati disattivati i cookie di terzi (generalmente attivati per impostazione predefinita in quasi tutti i browser), è necessario accettarli per consentire il corretto funzionamento di Salesforce. Se gli utenti dispongono di accesso generalizzato a Internet, non è necessario eseguire alcuna operazione.

# Il menu Imposta

## Interfaccia utente Imposta migliorata in Salesforce Classic

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **tutte** le versioni tranne **Database.com** Edition

L'interfaccia utente Imposta migliorata fornisce un'esperienza semplificata per la visualizzazione e la gestione delle operazioni di impostazione personale e amministrativa.

Quando in un'organizzazione è abilitata l'interfaccia utente Imposta migliorata, è possibile notare numerose differenze rispetto all'interfaccia utente originale.

- Il menu Imposta è accessibile dal link Imposta nell'angolo superiore destro di tutte le pagine Salesforce.

- Il menu Imposta è organizzato i categorie basate sugli obiettivi: Amministra, Crea, Distribuisci, Monitora e Checkout.
- Le impostazioni personali, che tutti gli utenti di Salesforce possono modificare, sono disponibili da un menu Impostazioni personali separato.

  Per accedere alle Impostazioni personali, selezionare il proprio nome nell'angolo superiore destro di qualsiasi pagina Salesforce, quindi fare clic su **Impostazioni personali**. È anche possibile accedere alla Impostazioni personali dalla pagina del profilo Chatter personale: nel riquadro destro, fare clic su **Impostazioni personali**.
- La pagina iniziale Impostazioni personali include link rapidi per accedere facilmente agli strumenti e alle operazioni delle impostazioni personali utilizzati più di frequente.

Importante: Quando è abilitata, l'interfaccia utente Imposta migliorata è attivata per tutti gli utenti dell'organizzazione. Assicurarsi di informare la propria organizzazione prima di abilitare o disabilitare questa impostazione.

Per abilitare l'interfaccia utente Imposta migliorata, da Imposta, immettere `Interfaccia utente` nella casella `Ricerca veloce`, quindi selezionare **Interfaccia utente** e **Abilita interfaccia utente Imposta migliorata**.

Nota: L'interfaccia utente migliorata:

- non è supportata in Internet Explorer versione 6
- è disponibile solo quando viene abilitato il nuovo tema dell'interfaccia utente

## Ricerca nell'impostazione con la Ricerca avanzata in Imposta (beta)

Con la Ricerca avanzata in Imposta, gli utenti possono cercare molti tipi di elementi in Imposta, incluse voci di approvazione, oggetti e campi personalizzati, profili personalizzati, insiemi di autorizzazioni, voci di flusso di lavoro, utenti, e così via.

Nota: La Ricerca avanzata in Imposta è in versione beta. Presenta una qualità pari all'istanza di produzione ma con limitazioni note.

Per utilizzare la Ricerca avanzata in Imposta, accertarsi che la relativa impostazione dell'interfaccia utente sia abilitata. Da Imposta, immettere `Interfaccia utente` nella casella `Ricerca veloce`, quindi selezionare **Interfaccia utente** e scorrere fino a `Abilita interfaccia utente Imposta migliorata (beta)`. Se la Ricerca avanzata in Imposta è disabilitata, la casella di ricerca in Imposta restituisce soltanto i titoli delle pagine nel menu Imposta, non le singole voci eventualmente create o modificate in Imposta.

La Ricerca avanzata in Imposta è polivalente e consente diversi usi.

- Per trovare le pagine di Imposta, digitare in parte o completamente il nome di una pagina nella casella della ricerca in Imposta. Man mano che si digita testo nella casella, appaiono immediatamente le pagine di Imposta i cui nomi corrispondono al testo digitato. Fare clic sul nome della pagina da aprire.
- Per trovare metadati in Imposta, immettere almeno due caratteri consecutivi della voce desiderata e fare clic su o premere Invio. Nella pagina Risultati della ricerca impostazione visualizzata, selezionare l'elemento desiderato dall'elenco.

  Nota: Alcuni elementi per i quali si può eseguire la ricerca (come gli insiemi di autorizzazioni) non sono disponibili in alcune versioni. Gli utenti non possono cercare elementi che non sono inclusi nella versione in uso.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per abilitare la Ricerca avanzata in Imposta:
- "Personalizza applicazione"

Per eseguire una ricerca in Imposta:
- "Visualizza impostazione e configurazione"

Esempio: Ad esempio, si supponga di voler visualizzare tutti i pacchetti installati nella propria organizzazione. Immettere `inst`. Man mano che si immettono le lettere, il menu Imposta si riduce in modo da includere solo i menu e le pagine che corrispondono ai termini della ricerca. Apparirà rapidamente il link per la pagina desiderata (**Pacchetti installati**).

Quindi, si può ad esempio modificare la password di uno degli utenti, Jane Smith. Immettere `smit` e fare clic su . Nella pagina Risultati ricerca impostazione, fare clic sul risultato Jane Smith per passare direttamente alla pagina dei dettagli dell'utente.

VEDERE ANCHE:

Pagina Risultati di ricerca impostazione (beta)

## Pagina Risultati di ricerca impostazione (beta)

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

La pagina Risultati di ricerca impostazione visualizza diversi tipi di elementi in Imposta corrispondenti ai termini della ricerca, incluse voci di approvazione, oggetti e campi personalizzati, profili personalizzati, insiemi di autorizzazioni, voci di flusso di lavoro, utenti, e così via.

Nota: La Ricerca avanzata in Imposta è in versione beta. Presenta una qualità pari all'istanza di produzione ma con limitazioni note.

Nella pagina Risultati di ricerca impostazione:

- Nel riquadro sinistro sono indicate tutte le categorie con il numero di risultati tra parentesi.
  - Fare clic su una categoria per visualizzare solo i risultati relativi a quella categoria.
  - Se i risultati sono stati filtrati per categoria, fare clic su **Tutti i risultati** per visualizzare tutti i risultati della ricerca.
- Fare clic su un risultato per aprirlo o fare clic su **Modifica**.
- Utilizzare la casella di ricerca nella parte superiore della pagina per eseguire di nuovo una ricerca impostazione.

Nota: I termini della ricerca che soddisfano un nome utente o un nickname della comunità (il campo `Nickname` nella pagina dei dettagli dell'utente) restituiscono i risultati che mostrano solo il nome dell'utente. Se il nickname non corrisponde al nome utente, il risultato potrebbe non essere scontato. Ad esempio, se un'utente di nome Margherita Rossi ha il nickname Margy, la ricerca di `mar` restituisce Margherita Rossi.

Suggerimento: quando si visualizzano i risultati della ricerca impostazione, creare un segnalibro per la pagina dei risultati nel browser Web per semplificare l'esecuzione della stessa ricerca in futuro. Ad esempio, se si cerca spesso la parola "smit", è possibile creare un segnalibro per la pagina dei risultati in modo che esegua di nuovo la stessa ricerca. L'URL per questo segnalibro sarebbe di questo tipo:
`https://MiaSocietà.salesforce.com/ui/setup/SetupSearchResultsPage?setupSearch=smit`.

VEDERE ANCHE:

Ricerca nell'impostazione con la Ricerca avanzata in Imposta (beta)

# Lingua, impostazioni internazionali e valuta

Le impostazioni di Salesforce per lingua, impostazioni internazionali, fuso orario e valuta possono influire sulle modalità di visualizzazione degli oggetti (account, lead, opportunità e simili). In un'organizzazione con una sola valuta, gli amministratori di Salesforce definiscono le impostazioni internazionali della valuta, la lingua predefinita, le impostazioni internazionali predefinite e il fuso orario predefinito per le rispettive organizzazioni e gli utenti possono definire una lingua, delle impostazioni internazionali e un fuso orario personali nelle pagine delle impostazioni personali. In un'organizzazione con più valute, gli amministratori di Salesforce definiscono la valuta aziendale, la lingua predefinita, le impostazioni internazionali predefinite e il fuso orario predefinito per le rispettive organizzazioni e gli utenti possono definire una valuta, una lingua, delle impostazioni internazionali e un fuso orario personali nella pagine delle impostazioni personali.

Nota: le organizzazioni con una sola lingua non possono modificare la lingua, ma possono modificare le impostazioni internazionali.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

| Impostazione | Chi può modificare l'impostazione |
| --- | --- |
| `Valuta` | Utente di un'organizzazione con più valute |
| `Valuta aziendale` | Amministratore di un'organizzazione con più valute |
| `Impostazioni internazionali valuta` | Amministratore di un'organizzazione con una sola valuta |
| `Codice ISO predefinito valuta` | Non modificabile |
| `Lingua predefinita` | Amministratore |
| `Impostazioni internazionali predefinite` | Amministratore |
| `Fuso orario predefinito` | Amministratore |
| `Valuta informazioni` | Non modificabile |
| `Lingua` | Utente |
| `Impostazioni internazionali` | Utente |
| `Fuso orario` | Utente |

VEDERE ANCHE:

Panoramica sulle impostazioni relative alla lingua
Valute supportate
Quali lingue supporta Salesforce?
Impostazioni internazionali supportate
Fusi orari supportati
Impostazione della valuta personale o della propria organizzazione

# Panoramica sulle impostazioni relative alla lingua

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **tutte** le versioni tranne **Database.com** Edition

L'interfaccia utente Web di Salesforce, Salesforce per Outlook, Connect Offline e Connect per Office è disponibile in più lingue.

L'interfaccia utente Web di Salesforce dispone di due impostazioni relative alla lingua:

- Lingua personale: tutto il testo, le immagini, i pulsanti e la guida in linea vengono visualizzati in questa lingua. Per modificare questa impostazione, modificare le informazioni personali.
- Lingua predefinita dell'organizzazione: si applica a tutti i nuovi utenti finché non selezionano la propria lingua. Questa impostazione determina inoltre la lingua in cui vengono memorizzate tutte le personalizzazioni (campi personalizzati, schede e opzioni dell'interfaccia utente). Nel caso delle personalizzazioni, le lingue personali dei singoli utenti non sostituiscono questa impostazione. Alcuni elementi di impostazione immessi manualmente da un amministratore possono essere tradotti mediante l'Area di lavoro traduzione.

  Gli amministratori possono modificare questa impostazione modificando le informazioni sulla società.

Il testo immesso dagli utenti rimane nella lingua in cui è stato immesso.

VEDERE ANCHE:

Lingua, impostazioni internazionali e valuta

## Quali lingue supporta Salesforce?

Salesforce offre tre livelli di supporto linguistico: lingue interamente supportate, lingue dell'utente finale e lingue solo per la piattaforma. Ogni lingua è identificata da un codice lingua di due caratteri (ad esempio `en`) o da un codice impostazione internazionale di cinque caratteri (quale en_AU).

Oltre a utilizzare il supporto linguistico di Salesforce, è possibile localizzare le organizzazioni in due modi. L'Area di lavoro traduzione consente di specificare le lingue nelle quali si desidera tradurre, assegnare traduttori alle lingue, creare traduzioni per le personalizzazioni apportate alla propria organizzazione Salesforce e ignorare le etichette e le traduzioni dei pacchetti gestiti. Tutto è traducibile, dai valori degli elenchi di selezione personalizzati ai campi personalizzati, quindi gli utenti globali possono utilizzare l'intera organizzazione Salesforce nella propria lingua.

La seconda opzione è rinominare schede e campi in Salesforce. Se l'applicazione personalizzata utilizza solo alcune schede e campi standard di Salesforce, è possibile tradurli.

### Lingue interamente supportate

Per cambiare la lingua di tutte le funzionalità, inclusa la Guida, impostando una delle seguenti lingue interamente supportate, da Imposta, immettere *Informazioni sulla società* nella casella `Ricerca veloce`, selezionare **Informazioni sulla società** e quindi **Modifica**.

- Cinese (semplificato): `zh_CN`
- Cinese (tradizionale): `zh_TW`
- Danese: `da`
- Olandese: `nl_NL`
- Inglese: `en_US`
- Finlandese: `fi`
- Francese: `fr`

- Tedesco: de
- Italiano: it
- Giapponese: ja
- Coreano: ko
- Norvegese: no
- Portoghese (Brasile): pt_BR
- Russo: ru
- Spagnolo: es
- Spagnolo (Messico): es_MX
- Svedese: sv
- Tailandese: th

Nota:

- Spagnolo (Messico) viene trasformato in Spagnolo per le traduzioni definite dal cliente.
- Anche se l'interfaccia utente di Salesforce viene interamente tradotta in tailandese, la Guida resta in inglese.

## Lingue degli utenti finali

Le lingue degli utenti finali sono utili nel caso di un'organizzazione multilingue o di partner che parlano lingue diverse da quella predefinita della società. Per le lingue degli utenti finali, Salesforce è dotato di etichette tradotte per tutti gli oggetti standard e le pagine, *fatta eccezione* per le pagine amministrative, l'impostazione e la Guida. Quando si specifica una lingua utente finale, le etichette e la Guida non tradotte vengono visualizzate in inglese. Le lingue utente finale sono destinate esclusivamente all'uso personale da parte degli utenti finali. Non utilizzare le lingue utente finale come lingue aziendali. Salesforce non fornisce assistenza ai clienti nelle lingue utente finale.

Le lingue utente finale includono:

- Arabo: ar
- Bulgaro: bg
- Croato: hr
- Ceco: cs
- Inglese (Regno Unito): en_GB
- Greco: el
- Ebraico: iw
- Ungherese: hu
- Indonesiano: in
- Polacco: pl
- Portoghese (Portogallo): pt_PT
- Rumeno: ro
- Slovacco: sk
- Sloveno: sl
- Turco: tr
- Ucraino: uk
- Vietnamita: vi

Nota: Salesforce fornisce un supporto limitato per le lingue da destra a sinistra, ad esempio arabo ed ebraico, per le seguenti funzionalità.

- Live Agent
- Casi
- Account

Queste funzionalità sono supportate solo sul sito Salesforce completo (non su Salesforce1 o altri client mobili). Non si garantisce che le lingue da destra a sinistra funzionino correttamente con altre funzionalità Salesforce e non è previsto un ampliamento dell'elenco di funzionalità supportate.

Le funzionalità non supportate per le lingue da destra a sinistra includono, senza limitazione, le seguenti:

- Generatore di rapporti
- Generazione di preventivi in PDF
- Previsioni personalizzabili
- Email
- Salesforce Knowledge
- Feed
- Comunità

L'assenza di una funzionalità dall'elenco non implica la disponibilità del supporto. Con le lingue da destra a sinistra sono supportate solo le funzionalità Live Agent, Casi e Account.

## Lingue solo per la piattaforma

Nelle situazioni in cui Salesforce non fornisce traduzioni predefinite, utilizzare le lingue solo per la piattaforma per localizzare le applicazioni e personalizzare le funzionalità implementate nella piattaforma Salesforce1. È possibile tradurre elementi come etichette personalizzate, oggetti personalizzati e nomi di campi. È inoltre possibile rinominare la maggior parte di oggetti, etichette e campi standard. Il testo informativo e il testo delle etichette non relative ai campi non sono traducibili.

Le lingue solo per la piattaforma sono disponibili ovunque sia possibile selezionare una lingua nell'applicazione. Tuttavia, quando si seleziona una lingua solo per la piattaforma, tutte le etichette standard di Salesforce vengono automaticamente impostate sull'inglese o, in determinati casi, sulla lingua di un utente finale o una lingua completamente supportata.

Quando si specifica una lingua solo per la piattaforma, le etichette per gli oggetti e i campi standard restano in inglese tranne nei seguenti casi:

- Inglese (Australia), Inglese (India), Inglese (Malesia) e Inglese (Filippine) vengono trasformati in Inglese (Regno Unito).
- Tedesco (Austria) e Tedesco (Svizzera) vengono trasformati in Tedesco.
- Francese (Canada) viene trasformato in Francese.
- Rumeno (Moldavia) viene trasformato in Rumeno.
- Montenegrino viene trasformato in Serbo (Latino).
- Portoghese (Portogallo) viene trasformato in Portoghese (Brasile).

Attualmente sono supportate le seguenti lingue solo per la piattaforma.

- Albanese: `sq`
- Arabo (Algeria): `ar_DZ`
- Arabo (Bahrein): `ar_BH`
- Arabo (Egitto): `ar_EG`

- Arabo (Iraq): ar_IQ
- Arabo (Giordania): ar_JO
- Arabo (Kuwait): ar_KW
- Arabo (Libano): ar_LB
- Arabo (Libia): ar_LY
- Arabo (Marocco): ar_MA
- Arabo (Oman): ar_OM
- Arabo (Qatar): ar_QA
- Arabo (Arabia Saudita): ar_SA
- Arabo (Sudan): ar_SD
- Arabo (Siria): ar_SY
- Arabo (Tunisia): ar_TN
- Arabo (Emirati Arabi Uniti): ar_AE
- Arabo (Yemen): ar_YE
- Armeno: hy
- Basco: eu
- Bosniaco: bs
- Bengalese: bn
- Cinese (semplificato-Singapore): zh_SG
- Cinese (tradizionale-Hong Kong): zh_HK
- Inglese (Australia): en_AU
- Inglese (Canada): en_CA
- Inglese (Hong Kong): en_HK
- Inglese (India): en_IN
- Inglese (Irlanda): en_IE
- Inglese (Malesia): en_MY
- Inglese (Filippine): en_PH
- Inglese (Singapore): en_SG
- Inglese (Sud Africa): en_ZA
- Estone: et
- Francese (Belgio): fr_BE
- Francese (Canada): fr_CA
- Francese (Lussemburgo): fr_LU
- Francese (Svizzera): fr_CH
- Georgiano: ka
- Tedesco (Austria): de_AT
- Tedesco (Lussemburgo): de_LU
- Tedesco (Svizzera): de_CH
- Hindi: hi
- Islandese: is

- Irlandese: `ga`
- Italiano (Svizzera): `it_CH`
- Lettone: `lv`
- Lituano: `lt`
- Lussemburghese: `lb`
- Macedone: `mk`
- Malese: `ms`
- Maltese: `mt`
- Rumeno (Moldavia): `ro_MD`
- Montenegrino: `sh_ME`
- Romancio: `rm`
- Serbo (Cirillico): `sr`
- Serbo (Latino): `sh`
- Spagnolo (Argentina): `es_AR`
- Spagnolo (Bolivia): `es_BO`
- Spagnolo (Cile): `es_CL`
- Spagnolo (Colombia): `es_CO`
- Spagnolo (Costa Rica): `es_CR`
- Spagnolo (Repubblica Dominicana): `es_DO`
- Spagnolo (Ecuador): `es_EC`
- Spagnolo (El Salvador): `es_SV`
- Spagnolo (Guatemala): `es_GT`
- Spagnolo (Honduras): `es_HN`
- Spagnolo (Nicaragua): `es_NI`
- Spagnolo (Panama): `es_PA`
- Spagnolo (Paraguay): `es_PY`
- Spagnolo (Perù): `es_PE`
- Spagnolo (Porto Rico): `es_PR`
- Spagnolo (Stati Uniti): `es_US`
- Spagnolo (Uruguay): `es_UY`
- Spagnolo (Venezuela): `es_VE`
- Tagalog: `tl`
- Tamil: `ta`
- Urdu: `ur`
- Gallese: `cy`

VEDERE ANCHE:

Lingua, impostazioni internazionali e valuta

## Impostazioni internazionali supportate

Le impostazioni internazionali di Salesforce determinano i formati di visualizzazione per data e ora, nomi degli utenti, indirizzi, virgole e punti nei numeri. Per le organizzazioni con una sola valuta, le impostazioni internazionali determinano anche la valuta predefinita per l'organizzazione quando vengono selezionate nell'elenco di selezione `Impostazioni internazionali valuta` nella pagina Informazioni sulla società.

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Albanese (Albania) | sq_AL | Lek (Albania): ALL | 28.02.08 4.30.PM | 6.00.PD | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1, Riga indirizzo 2 Città, Stato Codice postale Paese |
| Arabo (Algeria) | ar_DZ | Dinaro (Algeria): DZD | 28/02/2008 04:30 PM | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1, Riga indirizzo 2 Città, Stato Codice postale Paese |
| Arabo (Bahrein) | ar_BH | Dinaro del Bahrein: BHD | 28/02/2008 04:30 PM | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1, Riga indirizzo 2 Città, Stato Codice postale Paese |
| Arabo (Egitto) | ar_EG | Lira egiziana (Egitto): EGP | 28/02/2008 04:30 PM | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1, Riga indirizzo 2 |

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Database.com Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le informazioni sulla società:
- "Visualizza impostazione e configurazione"

Per modificare le informazioni sulla società:
- "Personalizza applicazione"

Le opzioni di impostazione personale disponibili variano a seconda della versione di Salesforce utilizzata.

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
| --- | --- | --- | --- | --- | --- | --- | --- |
| | | | | | | | Città, Stato Codice postale<br>Paese |
| Arabo (Iraq) | ar_IQ | Dinaro (Iraq): IQD | 28/02/2008 04:30 PM | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Arabo (Giordania) | ar_JO | Dinaro giordano: JOD | 28/02/2008 04:30 PM | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Arabo (Kuwait) | ar_KW | Dinaro kuwaitiano: KWD | 28/02/2008 04:30 PM | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Arabo (Libano) | ar_LB | Sterlina libanese: LBP | 28/02/2008 04:30 PM | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Arabo (Libia) | ar_LY | Dinar (Libia): LYD | 28/02/2008 04:30 PM | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| Arabo (Marocco) | ar_MA | Dirham marocchino: MAD | 28/02/2008 04:30 PM | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Arabo (Oman) | ar_OM | Rial (Oman): OMR | 28/02/2008 04:30 PM | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Arabo (Qatar) | ar_QA | Rial (Qatar): QAR | 28/02/2008 04:30 PM | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Arabo (Arabia Saudita) | ar_SA | Riyal saudita: SAR | 28/02/2008 04:30 PM | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Arabo (Sudan) | ar_SD | Sterlina sudanese: SDG | 28/02/2008 04:30 PM | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Arabo (Siria) | ar_SY | Lira (Siria): SYP | 28/02/2008 04:30 PM | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| | | | | | | | Paese |
| Arabo (Tunisia) | ar_TN | Dinaro (Tunisia): TND | 28/02/2008 04:30 PM | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Arabo (Emirati Arabi Uniti) | ar_AE | Dirham degli EAU: AED | 28/02/2008 04:30 PM | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Arabo (Yemen) | ar_YE | Riyal (Yemen): YER | 28/02/2008 04:30 PM | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Armeno (Armenia) | hy_AM | Dram armeno: AMD | 02/28/2008 16:30 | 06:00 | 1234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Azerbaigiano (Azerbaigian) | az_AZ | Nuovo manat (Azerbaigian): AZN | 2008-02-28 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Basco (Spagna) | eu_ES | Euro: EUR | 2008-02-28 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2 |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| | | | | | | | Città, Stato Codice postale<br>Paese |
| Bielorusso (Bielorussia) | be_BY | Rublo (Bielorussia): BYR | 28.2.2008 16.30 | 6.00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Bengalese (Bangladesh) | bn_BD | Taka (Bangladesh): BDT | / / : PM | : | , . | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Bosniaco (Bosnia ed Erzegovina) | bs_BA | Marchi convertibili: BAM | 28.02.2008. 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Bulgaro (Bulgaria) | bg_BG | Lev (Bulgaria): BGN | 2008-2-28 16:30 | 6:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Burmese (Myanmar [Birmania]) | my_MM | Kyat (Myanmar): MMK | / / : | : | , . | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| Catalano (Spagna, Euro) | ca_ES_EURO | Euro: EUR | 28/02/2008 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Catalano (Spagna) | ca_ES | Euro: EUR | 28/02/2008 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Cinese (Cina, ordine Pinyin) | zh_CN_PINYIN | Yuan cinese: CNY | 28.02.08 PM4:30 | 上午 6:00 | 1,234.56 | Cognome Nome | Paese<br>Codice postale Stato Città<br>Riga indirizzo 1,<br>Riga indirizzo 2 |
| Cinese (Cina, ordine dei tratti) | zh_CN_STROKE | Yuan cinese: CNY | 28.02.08 PM4:30 | 上午6:00 | 1,234.56 | Cognome Nome | Paese<br>Codice postale Stato Città<br>Riga indirizzo 1,<br>Riga indirizzo 2 |
| Cinese (Cina) | zh_CN | Yuan cinese: CNY | 28.02.08 PM4:30 | 上午6:00 | 1,234.56 | Cognome Nome | Paese<br>Codice postale Stato Città<br>Riga indirizzo 1,<br>Riga indirizzo 2 |
| Cinese (Regione amministrativa speciale di Hong Kong, | zh_HK_STROKE | Dollaro di Hong Kong: HKD | 2008 2 28 PM4:30 | 6:00 | 1,234.56 | Cognome Nome | Paese<br>Codice postale Stato Città<br>Riga indirizzo 1, |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| ordine dei tratti) | | | | | | | Riga indirizzo 2 |
| Cinese (Regione amministrativa speciale di Hong Kong) | zh_HK | Dollaro di Hong Kong: HKD | 2008 2 28 PM4:30 | 6:00 | 1,234.56 | Cognome Nome | Paese<br>Codice postale Stato Città<br>Riga indirizzo 1,<br>Riga indirizzo 2 |
| Cinese (Regione amministrativa speciale di Macau) | zh_MO | Pataca (Macao): MOP | 2008 2 28 PM4:30 | 6:00 | 1,234.56 | Cognome Nome | Paese<br>Codice postale Stato Città<br>Riga indirizzo 1,<br>Riga indirizzo 2 |
| Cinese (Singapore) | zh_SG | Dollaro di Singapore: SGD | 28/02/2008 PM 04:30 | 06:00 | 1,234.56 | Cognome Nome | Paese<br>Codice postale Stato Città<br>Riga indirizzo 1,<br>Riga indirizzo 2 |
| Cinese (Taiwan, ordine dei tratti) | zh_TW_STROKE | Dollaro di Taiwan: TWD | 2008-2-28 PM 4:30 | 上午 06:00:00 | 1,234.56 | Cognome Nome | Paese<br>Codice postale Stato Città<br>Riga indirizzo 1,<br>Riga indirizzo 2 |
| Cinese (Taiwan) | zh_TW | Dollaro di Taiwan: TWD | 2008-2-28 PM 4:30 | 上午 06:00:00 | 1,234.56 | Cognome Nome | Paese<br>Codice postale Stato Città<br>Riga indirizzo 1,<br>Riga indirizzo 2 |
| Croato (Croazia) | hr_HR | Kuna croato: HRK | 28.02.2008. 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2 |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| | | | | | | | Città, Stato Codice postale<br>Paese |
| Ceco (Repubblica Ceca) | cs_CZ | Corona ceca: CZK | 28.2.2008 16:30 | 6:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Danese (Danimarca) | da_DK | Corona danese: DKK | 28-02-2008 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Olandese (Aruba) | nl_AW | Fiorino (Aruba): AWG | 28-2-2008 16:30 | 6:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Olandese (Belgio) | nl_BE | Euro: EUR | 28/02/2008 16:30 | 6:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Olandese (Olanda) | nl_NL | Euro: EUR | 28-2-2008 16:30 | 6:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Olandese (Suriname) | nl_SR | Dollaro Suriname: SRD | 28-2-2008 16:30 | 6:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Dzongkha (Bhutan) | dz_BT | Ngultrum (Bhutan): BTN | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Antigua e Barbuda) | en_AG | Dollaro (Caraibi orientali): XCD | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Australia) | en_AU | Dollaro australiano: AUD | 28/02/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Bahamas) | en_BS | Dollaro (Bahamas): BSD | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Barbados) | en_BB | Dollaro delle Barbados: BBD | 28/02/2008 16:30 | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| | | | | | | | Paese |
| Inglese (Belize) | en_BZ | Dollaro (Belize): BZD | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Bermuda) | en_BM | Dollaro delle Bermuda: BMD | 28/02/2008 16:30 | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Botswana) | en_BW | Pula (Botswana): BWP | 28/02/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Camerun) | en_CM | Franco CFA (BEAC): XAF | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Canada) | en_CA | Dollaro canadese: CAD | 28/02/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Isole Cayman) | en_KY | Dollaro (Isole Cayman): KYD | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2 |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| | | | | | | | Città, Stato Codice postale<br>Paese |
| Inglese (Eritrea) | en_ER | Nakfa (Eritrea): ERN | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Isole Falkland) | en_FK | Sterlina (Isole Falkland): FKP | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Fiji) | en_FJ | Dollaro (Fiji): FJD | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Gambia) | en_GM | Dalasi (Gambia): GMD | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Ghana) | en_GH | Cedi ghanese: GHS | 28/02/2008 16:30 | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| Inglese (Gibilterra) | en_GI | Sterlina (Gibilterra): GIP | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Guyana) | en_GY | Dollaro (Guyana): GYD | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Regione amministrativa speciale di Hong Kong) | en_HK | Dollaro di Hong Kong: HKD | 28/2/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (India) | en_IN | Rupia (India): INR | 28/2/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Indonesia) | en_ID | Rupia indonesiana: IDR | 28/02/2008 16:30 | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Irlanda, Euro) | en_IE_EURO | Euro: EUR | 28/02/2008 16:30 | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| | | | | | | | Paese |
| Inglese (Irlanda) | en_IE | Euro: EUR | 28/02/2008 16:30 | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Giamaica) | en_JM | Dollaro (Giamaica): JMD | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Kenya) | en_KE | Scellino (Kenia): KES | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Liberia) | en_LR | Dollaro (Liberia): LRD | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Madagascar) | en_MG | Ariary malgascio: MGA | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Malawi) | en_MW | Kwacha (Malawi): MWK | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2 |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| | | | | | | | Città, Stato Codice postale<br>Paese |
| Inglese (Malesia) | en_MY | Ringgit malese: MYR | 28/02/2008 16:30 | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Mauritius) | en_MU | Rupia (Mauritius): MUR | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Namibia) | en_NA | Dollaro (Namibia): NAD | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Nuova Zelanda) | en_NZ | Dollaro neozelandese: NZD | 28/02/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Nigeria) | en_NG | Naira nigeriano: NGN | 28/02/2008 16:30 | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| Inglese (Pakistan) | en_PK | Rupia pakistana: PKR | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Papua Nuova Guinea) | en_PG | Kina (Papua Nuova Guinea): PGK | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Filippine) | en_PH | Peso (Filippine): PHP | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Ruanda) | en_RW | Franco (Ruanda): RWF | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (St Elena) | en_SH | Sterlina (St Elena): SHP | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Samoa) | en_WS | Tala (Samoa): WST | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| | | | | | | | Paese |
| Inglese (Seychelles) | en_SC | Rupia (Seychelles): SCR | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Sierra Leone) | en_SL | Leone (Sierra Leone): SLL | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Singapore) | en_SG | Dollaro di Singapore: SGD | 28/02/2008 16:30 | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese [Sint Maarten (parte olandese)] | en_SX | Fiorino (Antille Olandesi): ANG | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Isole Salomone) | en_SB | Dollaro (Isole Salomone): SBD | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Sud Africa) | en_ZA | Rand sudafricano: ZAR | 2008/02/28 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2 |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| | | | | | | | Città, Stato Codice postale<br>Paese |
| Inglese (Swaziland) | en_SZ | Lilangeni (Swaziland): SZL | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Tanzania) | en_TZ | Scellino (Tanzania): TZS | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Tonga) | en_TO | Pa'anga tongano: TOP | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Trinidad e Tobago) | en_TT | Dollaro di Trinidad e Tobago: TTD | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Uganda) | en_UG | Scellino (Uganda): UGX | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| Inglese (Regno Unito) | en_GB | Lira sterlina: GBP | 28/02/2008 16:30 | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Stati Uniti) | en_US | Dollaro U.S.A.: USD | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Inglese (Vanuatu) | en_VU | Vatu (Vanuatu): VUV | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Estone (Estonia) | et_EE | Euro: EUR | 28.02.2008 16:30 | 6:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Finlandese (Finlandia, Euro) | fi_FI_EURO | Euro: EUR | 28.2.2008 16:30 | 6:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Finlandese (Finlandia) | fi_FI | Euro: EUR | 28.2.2008 16:30 | 6:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| | | | | | | | Paese |
| Francese (Belgio) | fr_BE | Euro: EUR | 28/02/2008 16:30 | 6:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Francese (Canada) | fr_CA | Dollaro canadese: CAD | 2008-02-28 16:30 | 06:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Francese (Comore) | fr_KM | Franco (Comore): KMF | 28/02/2008 16:30 | 06:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Francese (Francia, Euro) | fr_FR_EURO | Euro: EUR | 28/02/2008 16:30 | 06:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Francese (Francia) | fr_FR | Euro: EUR | 28/02/2008 16:30 | 06:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Francese (Guinea) | fr_GN | Franco guineano (Guinea): GNF | 28/02/2008 16:30 | 06:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2 |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| | | | | | | | Città, Stato Codice postale<br>Paese |
| Francese (Guinea) | fr_HT | Gourde (Haiti): HTG | 28/02/2008 16:30 | 06:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Francese (Lussemburgo) | fr_LU | Euro: EUR | 28/02/2008 16:30 | 06:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Francese (Mauritania) | fr_MR | Ouguiya (Mauritania): MRO | 28/02/2008 16:30 | 06:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Francese (Monaco) | fr_MC | Euro: EUR | 28/02/2008 16:30 | 06:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Francese (Svizzera) | fr_CH | Franco svizzero: CHF | 28.02.2008 16:30 | 06:00 | 1'234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città<br>Paese - Codice postale stato |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Francese (Wallis e Futuna) | fr_WF | Franco (Pacifico): XPF | 28/02/2008 16:30 | 06:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Georgiano (Georgia) | ka_GE | Lari (Georgia): GEL | 2008-02-28 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Tedesco (Austria, Euro) | de_AT_EURO | Euro: EUR | 28.02.2008 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Codice postale Città<br>Stato Paese |
| Tedesco (Austria) | de_AT | Euro: EUR | 28.02.2008 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Codice postale Città<br>Stato Paese |
| Tedesco (Germania, Euro) | de_DE_EURO | Euro: EUR | 28.02.2008 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Codice postale Città<br>Stato Paese |
| Tedesco (Germania) | de_DE | Euro: EUR | 28.02.2008 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Codice postale Città |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| | | | | | | | Stato Paese |
| Tedesco (Lussemburgo, Euro) | de_LU_EURO | Euro: EUR | 28.02.2008 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Codice postale Città<br>Stato Paese |
| Tedesco (Lussemburgo) | de_LU | Euro: EUR | 28.02.2008 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Codice postale Città<br>Stato Paese |
| Tedesco (Svizzera) | de_CH | Franco svizzero: CHF | 28.02.2008 16:30 | 06:00 | 1'234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Codice postale Città<br>Stato Paese |
| Greco (Grecia) | el_GR | Euro: EUR | 28/2/2008 4:30 PM | 6:00 πμ | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Ebraico (Israele) | iw_IL | Shekel israeliano: ILS | 16:30 28/02/2008 | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Hindi (India) | hi_IN | Rupia (India): INR | / / : PM | : | , . | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2 |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| | | | | | | | Città, Stato Codice postale<br>Paese |
| Ungherese (Ungheria) | hu_HU | Forint ungherese: HUF | 2008.02.28. 16:30 | 6:00 | 1 234,56 | Cognome Nome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Islandese (Islanda) | is_IS | Corona islandese: ISK | 28.2.2008 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Indonesiano (Indonesia) | in_ID | Rupia indonesiana: IDR | 28/02/2008 16:30 | 6:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Irlandese (Irlanda) | ga_IE | Euro: EUR | 28/02/2008 16:30 | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Italiano (Italia) | it_IT | Euro: EUR | 28/02/2008 16.30 | 6.00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| Italiano (Svizzera) | it_CH | Franco svizzero: CHF | 28.02.2008 16:30 | 06:00 | 1'234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città<br>Paese - Codice postale stato |
| Giapponese (Giappone) | ja_JP | Yen giapponese: JPY | 2008/02/28 16:30 | 6:00 | 1,234.56 | Cognome Nome | Paese<br>Codice postale Stato Città<br>Riga indirizzo 1,<br>Riga indirizzo 2 |
| Kazako (Kazakistan) | kk_KZ | Tenge kazako: KZT | 28.02.2008 16:30 | 06:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Khmer (Cambogia) | km_KH | Riel cambogiano: KHR | 28/2/2008, 16:30 | 6:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Kirghiz (Kyrgyzstan) | ky_KG | Som (Kyrgyzstan): KGS | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Coreano (Corea del Nord) | ko_KP | Won (Corea del Nord): KPW | 2008. 2. 28 PM 4:30 | 오전 6:00 | 1,234.56 | Cognome Nome | Paese<br>Codice postale Stato Città<br>Riga indirizzo 1, |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| | | | | | | | Riga indirizzo 2 |
| Coreano (Corea del Sud) | ko_KR | Won coreano: KRW | 2008. 2. 28 PM 4:30 | 오전 6:00 | 1,234.56 | Cognome Nome | Paese<br>Codice postale Stato Città<br>Riga indirizzo 1,<br>Riga indirizzo 2 |
| Laos (Laos) | lo_LA | Kip (Laos): LAK | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Lettone (Lettonia) | lv_LV | Euro: EUR | 28.02.2008 16:30 | 06:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Lituano (Lituania) | lt_LT | Euro: EUR | 2008.2.28 16.30 | 06.00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Luba-Katanga (Congo - Kinshasa) | lu_CD | Franco (Congo): CDF | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Lussemburghese (Lussemburgo) | lb_LU | Euro: EUR | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2 |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| | | | | | | | Città, Stato Codice postale<br>Paese |
| Macedone (Macedonia) | mk_MK | Dinaro (Macedonia): MKD | 28.2.2008 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Malese (Brunei) | ms_BN | Dollaro (Brunei): BND | 28/02/2008 4:30 PM | 6:00 AM | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Malese (Malesia) | ms_MY | Ringgit malese: MYR | 28/02/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Maltese (Malta) | mt_MT | Euro: EUR | 28/02/2008 16:30 | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Nepalese (Nepal) | ne_NP | Rupia (Nepal): NPR | - - : | : | , . | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| Norvegese (Norvegia) | no_NO | Corona norvegese: NOK | 28.02.2008 16:30 | 06:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Pashto (Afghanistan) | ps_AF | Afghani nuovo (Afghanistan): AFN | : / / | : | | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Persiano (Iran) | fa_IR | Rial (Iran): IRR | : / / | : | | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Polacco (Polonia) | pl_PL | Zloty (Polonia): PLN | 28.02.2008 16:30 | 06:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Portoghese (Angola) | pt_AO | Kwanza angolano: AOA | 28-02-2008 16:30 | 6:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Portoghese (Brasile) | pt_BR | Real brasiliano: BRL | 28/02/2008 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| | | | | | | | Paese |
| Portoghese (Capo Verde) | pt_CV | Escudo (Capo Verde): CVE | 28-02-2008 16:30 | 6:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Portoghese (Mozambico) | pt_MZ | Nuovo metical (Mozambico): MZN | 28/02/2008 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Portoghese (Portogallo) | pt_PT | Euro: EUR | 28-02-2008 16:30 | 6:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Portoghese (São Tomé e Príncipe) | pt_ST | Dobra (Sao Tomé): STD | 28-02-2008 16:30 | 6:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Rumeno (Moldavia) | ro_MD | Leu (Moldavia): MDL | 28.02.2008, 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Rumeno (Romania) | ro_RO | Leu rumeno (Nuovo): RON | 28.02.2008 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2 |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| | | | | | | | Città, Stato Codice postale<br>Paese |
| Romancio (Svizzera) | rm_CH | Franco svizzero: CHF | 28.02.2008 16:30 | 06:00 | 1’234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città<br>Paese - Codice postale stato |
| Rundi (Burundi) | rn_BI | Franco (Burundi): BIF | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Russo (Russia) | ru_RU | Rublo russo: RUB | 28.02.2008 16:30 | 6:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Serbo (Bosnia ed Erzegovina) | sr_BA | Marchi convertibili: BAM | 2008-02-28 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Serbo (Serbia) | sr_RS | Dinaro serbo: RSD | 28.2.2008. 16.30 | 06.00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| Serbo (Serbia e Montenegro) | sr_CS | Dinaro serbo: CSD | 28.2.2008. 16.30 | 06.00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Serbo-croato (Bosnia ed Erzegovina) | sh_BA | Dollaro U.S.A.: USD | 28.02.2008. 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Serbo-croato (Montenegro) | sh_ME | Dollaro U.S.A.: USD | 28.02.2008. 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Serbo-croato (Serbia e Montenegro) | sh_CS | Dollaro U.S.A.: USD | 28.02.2008. 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Slovacco (Slovacchia) | sk_SK | Euro: EUR | 28.2.2008 16:30 | 6:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Sloveno (Slovenia) | sl_SI | Euro: EUR | 28.2.2008 16:30 | 6:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| | | | | | | | Paese |
| Somalo (Gibuti) | so_DJ | Franco (Gibuti): DJF | 28/02/2008 4:30 PM | 6:00 sn. | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Somalo (Somalia) | so_SO | Scellino (Somalia): SOS | 28/02/2008 4:30 PM | 6:00 sn. | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Spagnolo (Argentina): | es_AR | Peso argentino: ARS | 28/02/2008 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Spagnolo (Bolivia) | es_BO | Boliviano boliviano: BOB | 28-02-2008 04:30 PM | 06:00:00 AM | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Spagnolo (Cile): | es_CL | Peso cileno: CLP | 28-02-2008 04:30 PM | 06:00 AM | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Spagnolo (Colombia): | es_CO | Peso colombiano: COP | 28/02/2008 04:30 PM | 06:00 AM | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2 |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
| --- | --- | --- | --- | --- | --- | --- | --- |
| | | | | | | | Città, Stato Codice postale<br>Paese |
| Spagnolo (Costa Rica) | es_CR | Colon costaricano: CRC | 28/02/2008 04:30 PM | 06:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Spagnolo (Cuba) | es_CU | Peso (Cuba): CUP | 28/02/2008 16:30 | 6:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Spagnolo (Repubblica Dominicana) | es_DO | Peso (Repubblica Dominicana): DOP | 02/28/2008 04:30 PM | 06:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Spagnolo (Ecuador) | es_EC | Dollaro U.S.A.: USD | 28/02/2008 04:30 PM | 06:00 AM | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Spagnolo (El Salvador) | es_SV | Colon salvadoregno (El Salvador): SVC | 02-28-2008 04:30 PM | 06:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| Spagnolo (Guatemala): | es_GT | Quetzal guatemalteco: GTQ | 28/02/2008 04:30 PM | 06:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Spagnolo (Honduras) | es_HN | Lempira honduregna: HNL | 02-28-2008 04:30 PM | 06:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Spagnolo (Messico) | es_MX | Peso (Messico): MXN | 28/02/2008 04:30 PM | 06:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Spagnolo (Nicaragua) | es_NI | Cordoba (Nicaragua): NIO | 02-28-2008 04:30 PM | 06:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Spagnolo (Panama) | es_PA | Balboa panamense: PAB | 02/28/2008 04:30 PM | 06:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Spagnolo (Paraguay) | es_PY | Guaranì paraguaiano: PYG | 28/02/2008 04:30 PM | 06:00 AM | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| | | | | | | | Paese |
| Spagnolo (Perù) | es_PE | Nuevo Sol peruviano: PEN | 28/02/2008 04:30 PM | 06:00 AM | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Spagnolo (Porto Rico) | es_PR | Dollaro U.S.A.: USD | 02-28-2008 04:30 PM | 06:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Spagnolo (Spagna, Euro) | es_ES_EURO | Euro: EUR | 28/02/2008 16:30 | 6:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Spagnolo (Spagna) | es_ES | Euro: EUR | 28/02/2008 16:30 | 6:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Spagnolo (Stati Uniti) | es_US | Dollaro U.S.A.: USD | 2/28/2008 4:30 PM | 6:00 a.m. | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Spagnolo (Uruguay) | es_UY | Nuovo peso uruguaiano: UYU | 28/02/2008 04:30 PM | 06:00 AM | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2 |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| | | | | | | | Città, Stato Codice postale<br>Paese |
| Spagnolo (Venezuela) | es_VE | Bolivar venezuelano forte: VEF | 28/02/2008 04:30 PM | 06:00 AM | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Svedese (Svezia) | sv_SE | Corona svedese: SEK | 2008-02-28 16:30 | 06:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Tagalog (Filippine) | tl_PH | Peso (Filippine): PHP | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Tagico (Tajikistan) | tg_TJ | Somoni tagico: TJS | 2/28/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Tamil (India) | ta_IN | Rupia (India): INR | 2-28-2008 4:30 PM | 6:00 am | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| Tamil (Sri Lanka) | ta_LK | Rupia (Sri Lanka): LKR | 2-28-2008 4:30 PM | 6:00 am | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Tailandese (Thailandia) | th_TH | Baht tailandese: THB | 28/2/2551, 16:30 น. | 6:00 น. | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Tigrinya (Etiopia) | ti_ET | Birr (Etiopia): ETB | 28/02/2008 4:30 PM | 6:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Turco (Turchia) | tr_TR | Lira turca (Nuova): TRY | 28.02.2008 16:30 | 06:00 | 1.234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Ucraino (Ucraina) | uk_UA | Grivna ucraina: UAH | 28.02.2008 16:30 | 6:00 | 1 234,56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Urdu (Pakistan) | ur_PK | Rupia pakistana: PKR | 28/2/2008 4:30 PM | 6:00 AM | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale |

| Nome | Codice | Valuta predefinita | Formato di data e ora | Formato delle ore | Formato dei numeri | Formato dei nomi | Formato degli indirizzi |
|---|---|---|---|---|---|---|---|
| | | | | | | | Paese |
| Usbeco (latino, Uzbekistan) | uz_LATN_UZ | Sum (Uzbekistan): UZS | 2008-02-28 16:30 | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Vietnamita (Vietnam) | vi_VN | Dong vietnamita: VND | 16:30 28/02/2008 | 06:00 | 1.234,56 | Cognome Nome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Gallese (Regno Unito) | cy_GB | Lira sterlina: GBP | 28/02/2008 16:30 | 06:00 | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |
| Yoruba (Benin) | yo_BJ | Franco CFA (BCEAO): XOF | 28/02/2008 4:30 PM | 6:00 Àár | 1,234.56 | Ms. Nome Cognome | Riga indirizzo 1,<br>Riga indirizzo 2<br>Città, Stato Codice postale<br>Paese |

VEDERE ANCHE:

Lingua, impostazioni internazionali e valuta

## Fusi orari supportati

L'elenco dei fusi orari e dei codici supportati da Salesforce per l'organizzazione è riportato nelle impostazioni personali dell'utente.

1. Dalle impostazioni personali, immettere *`Fuso orario`* nella casella `Ricerca veloce`, quindi selezionare **Lingua e fuso orario**. Se non si ottiene alcun risultato, immettere *`Informazioni personali`* nella casella `Ricerca veloce`, quindi selezionare **Informazioni personali**. Quindi, fare clic su **Modifica**.
2. Fare clic sull'elenco a discesa Fuso orario per l'elenco dei fusi orari supportati.

A titolo di riferimento, i fusi orari e i codici supportati da Salesforce (in ordine cronologico) sono i seguenti:

| Codice fuso orario | Nome fuso orario |
| --- | --- |
| GMT+14:00 | Ora delle Isole di Line (Pacifico/Kiritimati) |
| GMT+13:00 | Ora internazionale standard di Phoenix (Pacifico/Enderbury) |
| GMT+13:00 | Ora di Tonga (Pacifico/Tongatapu) |
| GMT+12:45 | Ora standard delle Isole Chatham (Pacifico/Chatham) |
| GMT+12:00 | Ora standard della Nuova Zelanda (Pacifico/Auckland) |
| GMT+12:00 | Ora delle Isole Figi (Pacifico/Figi) |
| GMT+12:00 | Ora di Petropavlovsk-Kamchatski (Asia/Kamchatka) |
| GMT+11:30 | Ora di Norfolk (Pacifico/Norfolk) |
| GMT+11:00 | Ora standard dell'Isola Lord Howe (Australia/Lord_Howe) |
| GMT+11:00 | Ora delle Isole Salomone (Pacifico/Guadalcanal) |
| GMT+10:30 | Ora standard dell'Australia centrale ((Australia del Sud) Australia/Adelaide) |
| GMT+10:00 | Ora standard dell'Australia orientale (Nuovo Galles del Sud) (Australia/Sydney) |
| GMT+10:00 | Ora standard dell'Australia orientale (Queensland) (Australia/Brisbane) |
| GMT+09:30 | Ora standard dell'Australia centrale (Territorio del Nord) (Australia/Darwin) |
| GMT+09:00 | Ora standard della Corea (Asia/Seul) |
| GMT+09:00 | Ora standard del Giappone (Asia/Tokyo) |
| GMT+08:00 | Ora di Hong Kong (Asia/Hong_Kong) |

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Database.com Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le informazioni sulla società:
- "Visualizza impostazione e configurazione"

Per modificare le informazioni sulla società:
- "Personalizza applicazione"

Le opzioni di impostazione personale disponibili variano a seconda della versione di Salesforce utilizzata.

| Codice fuso orario | Nome fuso orario |
|---|---|
| GMT+08:00 | Ora della Malesia (Asia/Kuala_Lumpur) |
| GMT+08:00 | Ora delle Filippine (Asia/Manila) |
| GMT+08:00 | Ora standard della Cina (Asia/Shanghai) |
| GMT+08:00 | Ora di Singapore (Asia/Singapore) |
| GMT+08:00 | Ora standard della Cina (Asia/Taipei) |
| GMT+08:00 | Ora standard dell'Australia occidentale (Australia/Perth) |
| GMT+07:00 | Ora dell'Indocina (Asia/Bangkok) |
| GMT+07:00 | Ora dell'Indocina (Asia/Ho_Chi_Minh) |
| GMT+07:00 | Ora dell'Indonesia occidentale (Asia/Giakarta) |
| GMT+06:30 | Ora del Myanmar (Asia/Rangoon) |
| GMT+06:00 | Ora del Bangladesh (Asia/Dacca) |
| GMT+05:45 | Ora del Nepal (Asia/Katmandu) |
| GMT+05:30 | Ora standard dell'India (Asia/Colombo) |
| GMT+05:30 | Ora standard dell'India (Asia/Calcutta) |
| GMT+05:00 | Ora del Pakistan (Asia/Karachi) |
| GMT+05:00 | Ora dell'Uzbekistan (Asia/Tashkent) |
| GMT+05:00 | Ora di Ekaterinburg (Asia/Ekaterinburg) |
| GMT+04:30 | Ora dell'Afghanistan (Asia/Kabul) |
| GMT+04:00 | Ora estiva dell'Azerbaijan (Asia/Baku) |
| GMT+04:00 | Ora standard del Golfo (Asia/Dubai) |
| GMT+04:00 | Ora della Georgia (Asia/Tbilisi) |
| GMT+04:00 | Ora dell'Armenia (Asia/Yerevan) |
| GMT+03:30 | Ora legale dell'Iran (Asia/Teheran) |
| GMT+03:00 | Ora dell'Africa orientale (Africa/Nairobi) |
| GMT+03:00 | Ora standard dell'Arabia (Asia/Baghdad) |
| GMT+03:00 | Ora standard dell'Arabia (Asia/Kuwait) |
| GMT+03:00 | Ora standard dell'Arabia (Asia/Riad) |
| GMT+03:00 | Ora standard di Mosca (Europa/Minsk) |
| GMT+03:00 | Ora standard di Mosca (Europa/Mosca) |
| GMT+03:00 | Ora estiva dell'Europa orientale (Africa/Cairo) |

| Codice fuso orario | Nome fuso orario |
| --- | --- |
| GMT+03:00 | Ora estiva dell'Europa orientale (Asia/Beirut) |
| GMT+03:00 | Ora legale di Israele (Asia/Gerusalemme) |
| GMT+03:00 | Ora estiva dell'Europa orientale (Europa/Atene) |
| GMT+03:00 | Ora estiva dell'Europa orientale (Europa/Bucarest) |
| GMT+03:00 | Ora estiva dell'Europa orientale (Europa/Helsinki) |
| GMT+03:00 | Ora estiva dell'Europa orientale (Europa/Istanbul) |
| GMT+02:00 | Ora standard del Sud Africa (Africa/Johannesburg) |
| GMT+02:00 | Ora estiva dell'Europa centrale (Europa/Amsterdam) |
| GMT+02:00 | Ora estiva dell'Europa centrale (Europa/Berlino) |
| GMT+02:00 | Ora estiva dell'Europa centrale (Europa/Bruxelles) |
| GMT+02:00 | Ora estiva dell'Europa centrale (Europa/Parigi) |
| GMT+02:00 | Ora estiva dell'Europa centrale (Europa/Praga) |
| GMT+02:00 | Ora estiva dell'Europa centrale (Europa/Roma) |
| GMT+01:00 | Ora estiva dell'Europa occidentale (Europa/Lisbona) |
| GMT+01:00 | Ora dell'Europa centrale (Africa/Algeri) |
| GMT+01:00 | Ora estiva Regno Unito (Europa/Londra) |
| GMT–01:00 | Ora di Capo Verde (Atlantico/Cape_Verde) |
| GMT+00:00 | Ora dell'Europa occidentale (Africa/Casablanca) |
| GMT+00:00 | Ora estiva irlandese (Europa/Dublino) |
| GMT+00:00 | Ora media di Greenwich (GMT) |
| GMT–00:00 | Ora estiva della Groenlandia Orientale (America/Scoresbysund) |
| GMT–00:00 | Ora estiva delle Azzorre (Atlantico/Azzorre) |
| GMT–02:00 | Ora standard della Georgia del sud (Atlantico/South_Georgia) |
| GMT–02:30 | Ora legale di Terranova (America/St_Johns) |
| GMT–03:00 | Ora estiva di Brasilia (America/Sao_Paulo) |
| GMT–03:00 | Ora dell'Argentina (America/Argentina/Buenos_Aires) |
| GMT–03:00 | Ora estiva del Cile (America/Santiago) |
| GMT–03:00 | Atlantic Daylight Time (America/Halifax) |
| GMT–04:00 | Atlantic Standard Time (America/Puerto_Rico) |
| GMT–04:00 | Atlantic Daylight Time (Atlantico/Bermuda) |

| Codice fuso orario | Nome fuso orario |
|---|---|
| GMT–04:30 | Ora del Venezuela (America/Caracas) |
| GMT–04:00 | Eastern Daylight Time (America/Indiana/Indianapolis) |
| GMT–04:00 | Eastern Daylight Time (America/New_York) |
| GMT–05:00 | Ora della Colombia (America/Bogotà) |
| GMT–05:00 | Ora del Perù (America/Lima) |
| GMT–05:00 | Eastern Standard Time (America/Panama) |
| GMT–05:00 | Central Daylight Time (America/Mexico_City) |
| GMT–05:00 | Central Daylight Time (America/Chicago) |
| GMT–06:00 | Central Standard Time (America/El_Salvador) |
| GMT–06:00 | Mountain Daylight Time (America/Denver) |
| GMT–06:00 | Mountain Standard Time (America/Mazatlan) |
| GMT–07:00 | Mountain Standard Time (America/Phoenix) |
| GMT–07:00 | Pacific Daylight Time (America/Los_Angeles) |
| GMT–07:00 | Pacific Daylight Time (America/Tijuana) |
| GMT–08:00 | Ora standard di Pitcairn (Pacifico/Pitcairn) |
| GMT–08:00 | Alaska Daylight Time (America/Anchorage) |
| GMT–09:00 | Ora di Gambier (Pacifico/Gambier) |
| GMT-9:00 | Hawaii-Aleutian Standard Time (America/Adak) |
| GMT–09:30 | Ora delle Isole Marchesi (Pacifico/Marchesi) |
| GMT-10:00 | Hawaii-Aleutian Standard Time (Pacific/Honolulu) |
| GMT-11:00 | Ora di Niue (Pacifico/Niue) |
| GMT-11:00 | Ora standard di Samoa (Pacifico/Pago_Pago) |

VEDERE ANCHE:

Lingua, impostazioni internazionali e valuta

# Impostazione della valuta personale o della propria organizzazione

Se si dispone di un'organizzazione con una sola valuta, è possibile impostare la valuta predefinita per l'organizzazione. Le organizzazioni con più valute non dispongono di una valuta predefinita. Invece, è possibile cambiare la valuta personale o aziendale.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le valute:
- "Visualizza impostazione e configurazione"

Per modificare le valute:
- "Personalizza applicazione"

IN QUESTA SEZIONE:

Impostazione delle impostazioni internazionali valuta
Se si dispone di un'organizzazione con una sola valuta, è possibile impostare la valuta predefinita.

Impostazione della valuta aziendale
Nelle organizzazioni con più valute, impostare la propria valuta aziendale sulla valuta in cui la sede centrale dell'organizzazione compila la dichiarazione dei redditi. Tutti i tassi di conversione si basano sulla valuta aziendale.

Impostazione della valuta personale
Nelle organizzazioni con più valute, gli utenti possono impostare una valuta personale diversa dalla valuta aziendale della loro organizzazione.

VEDERE ANCHE:

Lingua, impostazioni internazionali e valuta
Modifica dei tassi di conversione
Valute supportate
Impostazioni internazionali supportate

## Impostazione delle impostazioni internazionali valuta

Se si dispone di un'organizzazione con una sola valuta, è possibile impostare la valuta predefinita.

1. Cercare Imposta per Informazioni sulla società.
2. Nella pagina Informazioni sulla società, fare clic su **Modifica**.
3. Selezionare un'impostazione internazionale dall'elenco a discesa Impostazioni internazionali valuta.
4. Fare clic su **Salva**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le valute:
- "Visualizza impostazione e configurazione"

Per modificare le valute:
- "Personalizza applicazione"

## Impostazione della valuta aziendale

Nelle organizzazioni con più valute, impostare la propria valuta aziendale sulla valuta in cui la sede centrale dell'organizzazione compila la dichiarazione dei redditi. Tutti i tassi di conversione si basano sulla valuta aziendale.

Quando l'Assistenza abilita il supporto per più valute, la valuta aziendale è impostata sul valore specificato nella pagina Informazioni sulla società in Imposta. È possibile modificare la valuta aziendale.

1. Cercare Imposta per Gestisci valute.
2. Nella pagina Valuta, fare clic su **Cambia azienda**.
3. Selezionare una valuta dall'elenco a discesa Nuova valuta aziendale.
4. Fare clic su **Salva**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le valute:
- "Visualizza impostazione e configurazione"

Per modificare le valute:
- "Personalizza applicazione"

## Impostazione della valuta personale

Nelle organizzazioni con più valute, gli utenti possono impostare una valuta personale diversa dalla valuta aziendale della loro organizzazione.

1. Dalle impostazioni personali, immettere *Fuso orario* nella casella Ricerca veloce, quindi selezionare **Lingua e fuso orario**. Se non si ottiene alcun risultato, immettere *Informazioni personali* nella casella Ricerca veloce, quindi selezionare **Informazioni personali**.
2. Selezionare una valuta dall'elenco a discesa Valuta.
3. Salvare le modifiche.

EDIZIONI

Disponibile in: Salesforce Classic

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le informazioni sulla società:

- "Visualizza impostazione e configurazione"

Per modificare le informazioni sulla società:

- "Personalizza applicazione"

Le opzioni di impostazione personale disponibili variano a seconda della versione di Salesforce utilizzata.

## Modifica dei tassi di conversione

È possibile gestire i tassi di cambio statici tra le valute attive e inattive e la valuta aziendale modificando i tassi di conversione. Questi tassi di cambio vengono applicati a tutti i campi valutari utilizzati nell'organizzazione. Oltre a questi tassi di conversione, alcune organizzazioni utilizzano tassi di cambio datati per opportunità e prodotti opportunità.

EDIZIONI

Disponibile in: Salesforce Classic

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le valute:
- "Visualizza impostazione e configurazione"

Per modificare le valute:
- "Personalizza applicazione"

1. Cercare Imposta per Gestisci valute.
2. Se si utilizza la gestione avanzata delle valute, fare clic su **Gestisci valute**.
3. Fare clic su **Modifica tariffe** nell'elenco Valute attive o Valute inattive.
4. Immettere il tasso di conversione tra ogni valuta e la valuta aziendale.
5. Fare clic su **Salva**.

Quando si modificano i tassi di conversione, gli importi in valuta sono aggiornati con i nuovi tassi. I tassi di conversione precedenti non vengono memorizzati. Tutte le conversioni di opportunità, previsioni e altri importi utilizzano il tasso di conversione corrente.

Se l'organizzazione utilizza la gestione avanzata delle valute, è anche possibile gestire i tassi di cambio datati per i campi valutari delle opportunità e dei prodotti opportunità.

Nota:

- Non è possibile tenere traccia dei ricavi o delle perdite di bilancio sulla base delle fluttuazioni valutarie.
- La modifica dei tassi di conversione determina un ricalcolo globale dei campi di riepilogo di roll-up. Il ricalcolo potrebbe durare fino a 30 minuti, in base al numero di record interessati.
- È inoltre possibile modificare un tasso di conversione tramite API. Tuttavia, se è in corso un altro ricalcolo dei campi di riepilogo di roll-up, la durata di tale processo influisce sul processo di ricalcolo attivato. Di seguito viene descritto ciò che accade se si richiede una modifica del tasso di cambio tramite API mentre è in corso un processo correlato.
  - Se l'altro ricalcolo per lo stesso campo valuta è stato avviato meno di 24 ore fa, il tasso di cambio non viene salvato. È possibile ritentare in un secondo tempo o modificare il tasso di cambio da Gestisci valute in Imposta. L'avvio della modifica da Imposta interrompe il processo già in corso e attiva l'esecuzione del ricalcolo.
  - Se l'altro processo di ricalcolo è stato attivato più di 24 ore fa, è possibile salvare il tasso di cambio e il processo viene avviato.

Per verificare lo stato del processo di ricalcolo, consultare la pagina Processi in background in Imposta.

VEDERE ANCHE:

Impostazione della valuta personale o della propria organizzazione

## Valute supportate

Valute supportate da Salesforce:

| Nome valuta | Codice valuta |
|---|---|
| Dirham degli EAU | AED |
| Afghani nuovo (Afghanistan) | AFN |
| Lek albanese | ALL |
| Dram armeno | AMD |
| Fiorino delle Antille olandesi | ANG |
| Kwanza angolano | AOA |
| Peso argentino | ARS |
| Dollaro australiano | AUD |
| Fiorino di Aruba | AWG |
| Nuovo manat (Azerbaigian) | AZN |
| Marco convertibile | BAM |
| Dollaro delle Barbados | BBD |
| Taka del Bangladesh | BDT |
| Lev bulgaro | BGN |
| Dinaro del Bahrein | BHD |
| Franco burundese | BIF |
| Dollaro delle Bermuda | BMD |
| Dollaro del Brunei | BND |
| Boliviano boliviano | BOB |
| Mvdol boliviano | BOV |
| Cruzeiro brasiliano (vecchio) | BRB |
| Real brasiliano | BRL |
| Dollaro delle Bahamas | BSD |
| Ngultrum del Bhutan | BTN |
| Pula del Botswana | BWP |
| Rublo bielorusso | BYR |
| Dollaro belizeano | BZD |
| Dollaro canadese | CAD |

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Database.com Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le informazioni sulla società:

- "Visualizza impostazione e configurazione"

Per modificare le informazioni sulla società:

- "Personalizza applicazione"

Le opzioni di impostazione personale disponibili variano a seconda della versione di Salesforce utilizzata.

| Nome valuta | Codice valuta |
|---|---|
| Franco congolese | CDF |
| Franco svizzero | CHF |
| Unidades de fomento | CLF |
| Peso cileno | CLP |
| Yuan cinese | CNY |
| Peso colombiano | COP |
| Colon costaricano | CRC |
| Peso cubano | CUP |
| Escudo del Capo Verde | CVE |
| Corona ceca | CZK |
| Franco gibutiano | DJF |
| Corona danese | DKK |
| Peso dominicano | DOP |
| Dinaro algerino | DZD |
| Corona estone | EEK |
| Sterlina egiziana | EGP |
| Nakfa eritreo | ERN |
| Birr etiopico | ETB |
| Euro | EUR |
| Dollaro delle Figi | FJD |
| Sterlina delle Falkland | FKP |
| Lira sterlina | GBP |
| Lari georgiano | GEL |
| Cedi ghanese | GHS |
| Sterlina di Gibilterra | GIP |
| Dalasi gambiano | GMD |
| Franco della Guinea | GNF |
| Quetzal guatemalteco | GTQ |
| Dollaro della Guyana | GYD |
| Dollaro di Hong Kong | HKD |

| Nome valuta | Codice valuta |
|---|---|
| Lempira honduregna | HNL |
| Kuna croato | HRK |
| Gourde haitiano | HTG |
| Forint ungherese | HUF |
| Rupia indonesiana | IDR |
| Shekel israeliano | ILS |
| Rupia indiana | INR |
| Dinaro iracheno | IQD |
| Rial iraniano | IRR |
| Corona islandese | ISK |
| Dollaro giamaicano | JMD |
| Dinaro giordano | JOD |
| Yen giapponese | JPY |
| Scellino keniota | KES |
| Som chirghiso | KGS |
| Riel cambogiano | KHR |
| Franco comoriano | KMF |
| Won nordcoreano | KPW |
| Won coreano | KRW |
| Dinaro kuwaitiano | KWD |
| Dollaro delle Isole Cayman | KYD |
| Tenge kazako | KZT |
| Kip laotiano | LAK |
| Sterlina libanese | LBP |
| Rupia di Sri Lanka | LKR |
| Dollaro liberiano | LRD |
| Loti lesothiano | LSL |
| Dinaro libico | LYD |
| Dirham marocchino | MAD |
| Leu moldavo | MDL |

| Nome valuta | Codice valuta |
| --- | --- |
| Ariary malgascio | MGA |
| Dinaro macedone | MKD |
| Kyat birmano | MMK |
| Tugrik mongolo | MNT |
| Pataca di Macao | MOP |
| Ougulya mauritano | MRO |
| Rupia mauriziana | MUR |
| Rufiyaa delle Maldive | MVR |
| Kwacha malawiano | MWK |
| Peso messicano | MXN |
| Unidad de Inversion messicana (UDI) | MXV |
| Ringgit malese | MYR |
| Nuovo metical (Mozambico) | MZN |
| Dollaro namibiano | NAD |
| Naira nigeriano | NGN |
| Cordoba nicaraguense | NIO |
| Corona norvegese | NOK |
| Rupia nepalese | NPR |
| Dollaro neozelandese | NZD |
| Rial dell'Oman | OMR |
| Balboa panamense | PAB |
| Nuevo Sol peruviano | PEN |
| Kina Papua Nuova Guinea | PGK |
| Peso filippino | PHP |
| Rupia pakistana | PKR |
| Zloty polacco | PLN |
| Guaranì paraguaiano | PYG |
| Rial del Qatar | QAR |
| Leu rumeno (Nuovo) | RON |
| Dinaro serbo | RSD |

| Nome valuta | Codice valuta |
|---|---|
| Rublo russo | RUB |
| Franco ruandese | RWF |
| Riyal saudita | SAR |
| Dollaro delle Salomone | SBD |
| Rupia delle Seychelles | SCR |
| Sterlina sudanese | SDG |
| Corona svedese | SEK |
| Dollaro di Singapore | SGD |
| Sterlina di Sant'Elena | SHP |
| Leone della Sierra Leone | SLL |
| Scellino somalo | SOS |
| Dollaro Suriname | SRD |
| Sterlina del Sudan del Sud | SSP |
| Dobra di Sao Tomé | STD |
| Sterlina siriana | SYP |
| Lilangeni dello Swaziland | SZL |
| Baht tailandese | THB |
| Somoni tagico | TJS |
| Nuovo Manat del Turkmenistan | TMT |
| Dinaro tunisino | TND |
| Pa'anga tongano | TOP |
| Lira turca (Nuova) | TRY |
| Dollaro di Trinidad e Tobago | TTD |
| Dollaro di Taiwan | TWD |
| Scellino tanzaniano | TZS |
| Grivna ucraina | UAH |
| Scellino ugandese | UGX |
| Dollaro U.S.A. | USD |
| Nuovo peso uruguaiano | UYU |
| Sum uzbeko | UZS |

| Nome valuta | Codice valuta |
|---|---|
| Bolivar venezuelano forte | VEF |
| Dong vietnamita | VND |
| Vatu di Vanuatu | VUV |
| Tala samoano | WST |
| Franco CFA (BEAC) | XAF |
| Dollaro dei Caraibi Orientali | XCD |
| Franco CFA (BCEAO) | XOF |
| Franco CFP | XPF |
| Riyal yemenita | YER |
| Rand sudafricano | ZAR |
| Kwacha zambiano (Nuovo) | ZMK |
| Dollaro dello Zimbabwe | ZWL |

VEDERE ANCHE:

Impostazione della valuta personale o della propria organizzazione

# Informazioni sugli anni fiscali

Non tutte le aziende utilizzano l'anno gregoriano per il proprio anno fiscale. Salesforce facilita la definizione dell'anno fiscale che meglio si adatta alle specifiche esigenze aziendali.

Se l'anno fiscale scelto segue il calendario gregoriano, ma non inizia a gennaio, è possibile impostare facilmente il proprio anno fiscale definendo un anno fiscale standard. Se l'anno fiscale scelto segue una struttura diversa, è possibile definire un anno fiscale personalizzato che risponda al meglio alle proprie esigenze.

Sia che si utilizzi un anno fiscale standard o un anno fiscale personalizzato, è comunque possibile definire una volta anni fiscali individuali per l'intera organizzazione. Queste definizioni di anni fiscali consentono di utilizzare i periodi fiscali in tutti i componenti di Salesforce, inclusi rapporti, opportunità e previsioni.

Suggerimento: si suggerisce di definire il proprio anno fiscale personalizzato dopo la previsione corrente. Inoltre, è preferibile aggiornare le pianificazioni dei prodotti e le previsioni ogni volta che viene creato o modificato un anno fiscale personalizzato.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni tranne **Database.com** Edition.

AUTORIZZAZIONI UTENTE

Per definire o modificare gli anni fiscali:
- "Personalizza applicazione"

Per visualizzare gli anni fiscali:
- "Visualizza impostazione e configurazione"

## Anni fiscali standard

Gli anni fiscali standard sono periodi che seguono il calendario gregoriano, ma possono iniziare il primo giorno di qualsiasi mese dell'anno. A differenza dell'anno fiscale personalizzato, quello standard può essere utilizzato dalle organizzazioni che non dispongono della funzione di previsioni personalizzabili abilitata.

## Anni fiscali personalizzati

Per le aziende che suddividono i propri anni, trimestri e settimane fiscali in periodi fiscali personalizzati in base alle proprie esigenze di pianificazione finanziaria, Salesforce consente di definire con flessibilità tali periodi utilizzando gli anni fiscali personalizzati. Ad esempio, come parte di un anno fiscale personalizzato, è possibile creare un trimestre di 13 settimane rappresentato da tre periodi rispettivamente di 4, 4 e 5 settimane, anziché basarsi sui mesi del calendario.

Se si utilizza una struttura di anno fiscale tradizionale, come ad esempio 4-4-5 o una struttura a 13 periodi, è possibile definire rapidamente un anno fiscale specificando semplicemente una data iniziale e un modello incluso. Se la propria struttura di anno fiscale non è inclusa nei modelli, è possibile modificare facilmente un modello. Ad esempio, se si utilizzano tre trimestri fiscali all'anno (un quadrimestre) anziché quattro, eliminare o modificare i trimestri e i periodi in base alle proprie esigenze.

I periodi fiscali personalizzati possono essere rinominati in base ai propri standard. Ad esempio, un periodo fiscale potrebbe essere chiamato “P2” o “Febbraio".

Gli anni fiscali possono essere modificati ogni volta che si rende necessaria una modifica alla loro definizione. Ad esempio, si potrebbe aggiungere una settimana extra per sincronizzare un anno fiscale personalizzato con un calendario standard in un anno bisestile. Le modifiche alla struttura dell'anno fiscale sono effettive immediatamente dopo il salvataggio.

## Considerazioni sull'abilitazione degli anni fiscali personalizzati

Prima di abilitare gli anni fiscali personalizzati, prestare attenzione ai seguenti punti:

- Una volta abilitati, non è più possibile disabilitare gli anni fiscali personalizzati. Tuttavia, è possibile definire anni fiscali personalizzati che seguono la stessa struttura del calendario gregoriano degli anni fiscali standard di Salesforce.
- Gli anni fiscali non verranno creati automaticamente. Gli unici anni fiscali disponibili sono quelli definiti dalla propria organizzazione.
- Gli anni fiscali personalizzati possono essere abilitati solo con le previsioni personalizzabili, *non* con le previsioni collaborative.
- L'abilitazione o la definizione degli anni fiscali personalizzati influisce sulle previsioni, sui rapporti e sulle quote.
  - Quando si definisce un nuovo anno fiscale personalizzato o si modifica la durata di qualsiasi periodo fiscale, tutte le quote dell'anno andranno perse.
  - Quando si definisce un nuovo anno fiscale personalizzato oppure quando si modifica la durata di qualsiasi periodo fiscale, le previsioni, la cronologia delle previsioni e gli Ignora previsione andranno persi. La modifica della durata di un periodo fiscale potrebbe influire anche sull'anno fiscale precedente o successivo e sui rapporti associati ad esso. Le previsioni per i periodi precedenti al primo anno fiscale personalizzato verranno salvate e vi si potrà accedere normalmente.
  - I rapporti previsioni per un periodo successivo all'ultimo anno fiscale definito non possono essere raggruppati per periodo, ma solo per data.
  - Per assicurarsi che i rapporti previsioni presentino gli ammontare più aggiornati, visualizzare la previsione del periodo incluso nel rapporto prima di eseguire un rapporto previsione.
- La propria organizzazione non sarà in grado di utilizzare le colonne del periodo fiscale in rapporti opportunità, rapporti opportunità con prodotti o rapporti opportunità con pianificazioni.
- Le visualizzazioni elenco delle opportunità non includeranno le colonne di un periodo fiscale.

- Se sono abilitati gli anni fiscali personalizzati, non è possibile utilizzare le funzioni data `FISCAL_MONTH()`, `FISCAL_QUARTER()` oppure `FISCAL_YEAR()` in SOQL.

VEDERE ANCHE:

Impostazione dell'anno fiscale
Personalizzazione della struttura dell'anno fiscale
Personalizzazione delle etichette dell'anno fiscale
Selezione di un modello di anno fiscale personalizzato
Definizione di un anno fiscale personalizzato

# Impostazione dell'anno fiscale

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **tutte** le versioni tranne **Database.com** Edition.

AUTORIZZAZIONI UTENTE

Per visualizzare l'anno fiscale:
- "Visualizza impostazione e configurazione"

Per modificare l'anno fiscale:
- "Personalizza applicazione"

## Impostazione di un anno fiscale standard

Se l'organizzazione utilizza il calendario gregoriano, ma si desidera modificare il mese di inizio dell'anno fiscale, utilizzare anni fiscali standard. Gli anni fiscali standard possono iniziare il primo giorno di qualsiasi mese ed è possibile specificare se l'anno fiscale è denominato in base all'anno che inizia o a quello che finisce. Ad esempio, se l'anno fiscale inizia ad aprile 2015 e termina a marzo 2016, l'impostazione dell'anno fiscale può essere 2015 oppure 2016. Qualora l'anno fiscale sia più complesso, vedere Abilitazione degli anni fiscali personalizzati a pagina 69.

Avvertenza:

- Utenti delle previsioni personalizzabili: se si cambia il mese di inizio dell'anno fiscale è possibile che tutte le quote, la cronologia delle previsioni e le sovrascritture vadano perse. Per conservare i dati, impostare un mese utilizzato in precedenza come primo mese di un trimestre. Ad esempio, se il mese di inizio è aprile e si imposta il mese di maggio, mese con il quale non ha inizio alcun trimestre fiscale, i dati andranno persi. Se si imposta il mese di luglio, mese di inizio di un trimestre fiscale, i dati verranno conservati.
- Utenti delle previsioni collaborative: le informazioni relative alle quote e alle rettifiche vengono eliminate se si modifica il mese di inizio dell'anno fiscale.

Per impostare un anno fiscale standard:

1. Eseguire il backup dei dati attuali ed esportarli in un gruppo di file CSV.

   È consigliabile eseguire un'esportazione di backup dei dati poiché la modifica dell'anno fiscale provoca uno slittamento dei periodi fiscali. Questa modifica influisce su opportunità e previsioni a livello di organizzazione.

2. Da Imposta, immettere *`Anno fiscale`* nella casella `Ricerca veloce`, quindi selezionare **Anno fiscale**.
3. Selezionare `Anno fiscale standard`.
4. Scegliere il mese iniziale.
5. Specificare se il nome dell'anno fiscale è definito in base all'anno in cui inizia o in cui finisce.
6. Selezionare eventualmente `Applica a tutte le previsioni e quote` se si desidera applicare le nuove impostazioni dell'anno fiscale alle previsioni e alle quote esistenti. Questa opzione potrebbe non essere disponibile a seconda delle impostazioni delle previsioni.
7. Fare clic su **Salva**.

## Abilitazione degli anni fiscali personalizzati

Se l'organizzazione non utilizza un anno fiscale standard, è possibile abilitare anni fiscali personalizzati che consentono di definire in modo flessibile una struttura di anno fiscale più complessa.

Per abilitare gli anni fiscali personalizzati:

Nota: prima di abilitare gli anni fiscali personalizzati, assicurarsi di aver esportato eventuali dati relativi a periodi fiscali. Per informazioni specifiche sugli effetti dell'abilitazione degli anni fiscali personalizzati, vedere Informazioni sugli anni fiscali a pagina 66.

1. Eseguire il backup dei dati attuali ed esportarli in un gruppo di file CSV.

   È consigliabile eseguire un'esportazione di backup dei dati poiché la modifica dell'anno fiscale provoca uno slittamento dei periodi fiscali. Questa modifica influisce su opportunità e previsioni a livello di organizzazione.

2. Da Imposta, immettere *Anno fiscale* nella casella `Ricerca veloce`, quindi selezionare **Anno fiscale**.
3. Selezionare `Anno fiscale personalizzato`.
4. Fare clic su **Abilita anni fiscali personalizzati**.
5. Se si è consapevoli degli effetti dell'abilitazione degli anni fiscali personalizzati e si sono esportati tutti i dati, fare clic su **OK**.

   Avvertenza: una volta abilitati, non è più possibile disabilitare gli anni fiscali personalizzati. L'abilitazione degli anni fiscali personalizzati si ripercuote su rapporti, previsioni, quote e altre informazioni variabili in base alla data. Non abilitare gli anni fiscali personalizzati se non se ne conoscono le conseguenze e non si è preparati ad affrontarle.

6. Dopo aver abilitato gli anni fiscali personalizzati, definire il proprio anno fiscale. Vedere Definizione di un anno fiscale personalizzato a pagina 74.

# Personalizzazione della struttura dell'anno fiscale

Se il proprio anno fiscale personalizzato necessita di una struttura diversa rispetto a quella disponibile nei modelli, è possibile utilizzare una personalizzazione avanzata per modificarne i dettagli. Gli anni fiscali personalizzati consentono di:

- Personalizzare le etichette dei periodi
- Ripristinare l'anno fiscale alla struttura di un modello
- Aggiungere o rimuovere periodi fiscali
- Modificare la durata di una settimana fiscale

Avvertenza: la modifica della durata di un anno fiscale ha effetti anche sulle previsioni e i rapporti. Per informazioni dettagliate su tali effetti, vedere Informazioni sugli anni fiscali a pagina 67.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni tranne **Database.com** Edition.

AUTORIZZAZIONI UTENTE

Per definire o modificare gli anni fiscali:
- "Personalizza applicazione"

Per visualizzare gli anni fiscali:
- "Visualizza impostazione e configurazione"

## Personalizzazione delle etichette dei periodi

Le etichette dei periodi dell'anno fiscale per le previsioni e i rapporti sono impostate dai valori delle etichette predefiniti per i periodi dell'anno fiscale. Per modificarle, vedere Personalizzazione delle etichette dell'anno fiscale a pagina 71.

## Ripristino dell'anno fiscale alla struttura di un modello

Durante la personalizzazione, se si desidera tornare a un modello di anno fiscale, selezionare un modello dall'elenco a discesa `Ripristina struttura dell'anno fiscale`.

Nota: il ripristino della struttura dell'anno fiscale a un modello rimuove tutte le personalizzazioni apportate all'anno fiscale.

## Aggiunta o rimozione di periodi fiscali

È possibile aggiungere o rimuovere facilmente periodi fiscali (ad esempio, trimestri, periodi o settimane) dalla struttura dell'anno fiscale.

Per aggiungere periodi fiscali:

1. Da Imposta, immettere *Anno fiscale* nella casella `Ricerca veloce`, quindi selezionare **Anno fiscale**.
2. Fare clic su **Modifica** per l'anno fiscale che si desidera modificare.
3. Espandere la sezione **Personalizzazione avanzata** se non è ancora espansa.
4. Selezionare la casella di controllo del periodo prima del nuovo periodo. Ad esempio, se si desidera aggiungere un nuovo trimestre come secondo trimestre, selezionare la casella di controllo per il primo trimestre.
5. Fare clic su **Inserisci**.

   Nota: il numero massimo di periodi fiscali è 250.

Per rimuovere un periodo fiscale:

1. Da Imposta, immettere *Anno fiscale* nella casella `Ricerca veloce`, quindi selezionare **Anno fiscale**.
2. Fare clic su **Modifica** per l'anno fiscale che si desidera modificare.
3. Espandere la sezione **Personalizzazione avanzata** se non è ancora espansa.
4. Selezionare la casella di controllo del periodo che si desidera eliminare.
5. Fare clic su **Elimina**.

   Nota: è necessario che siano presenti almeno un trimestre, un periodo e una settimana.

## Modifica della durata di una settimana fiscale

Per modificare la durata dei periodi fiscali:

1. Da Imposta, immettere *Anno fiscale* nella casella `Ricerca veloce`, quindi selezionare **Anno fiscale**.
2. Fare clic su **Modifica** per l'anno fiscale che si desidera modificare.
3. Espandere la sezione **Personalizzazione avanzata** se non è ancora espansa.
4. Scegliere la durata dall'elenco a discesa **Durata** per la settimana fiscale.

   Nota: per modificare la durata di un periodo o di un trimestre fiscale, inserire o eliminare settimane o modificare la durata delle settimane che compongono il periodo o il trimestre.

Dopo aver personalizzato l'anno fiscale, visualizzare l'anteprima della relativa definizione. Se è corretta, chiudere l'anteprima e fare clic su **Salva** per salvare l'anno fiscale.

# Personalizzazione delle etichette dell'anno fiscale

È possibile personalizzare l'etichettatura dell'anno fiscale in due modi:

1. Assegnando un nome alle scelte di schemi e prefissi
2. Personalizzando gli elenchi di selezione dell'anno fiscale

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni tranne Database.com Edition.

AUTORIZZAZIONI UTENTE

Per definire o modificare gli anni fiscali:
- "Personalizza applicazione"

Per visualizzare gli anni fiscali:
- "Visualizza impostazione e configurazione"

## Assegnazione di un nome alle scelte di schemi e prefissi dell'anno fiscale

Quando si definisce un anno fiscale personalizzato, è possibile scegliere lo schema di etichettatura da utilizzare per il proprio anno fiscale personalizzato. Ciascun tipo di periodo fiscale (trimestre, periodo e settimana) presenta un elenco di schemi di etichettatura selezionabili.

**Schema nome trimestre**

**Numerato per anno**

Questa opzione consente di aggiungere il numero di trimestre all'etichetta del trimestre che è una combinazione dell'etichetta del prefisso e del numero del trimestre. Ad esempio, se il prefisso del trimestre è "T", l'etichetta del terzo trimestre sarà T3. Per personalizzare il prefisso del trimestre, vedere `Prefisso trimestre` a pagina 72. Per impostazione predefinita, il numero di ciascun trimestre è impostato in base al relativo ordine logico (ad esempio il primo trimestre è etichettato come "1"), ma è possibile personalizzarlo selezionando un valore diverso dall'elenco di selezione dei dettagli del trimestre.

**Nomi trimestre personalizzati**

Questa opzione consente di impostare l'etichetta del trimestre su qualsiasi nome. L'etichetta del trimestre viene impostata sul nome selezionato da `Nome trimestre`. Per impostazione predefinita l'ordine dei nomi dei trimestri è identico all'ordine dell'elenco di selezione, ma è possibile personalizzarlo selezionando un valore diverso dall'elenco a discesa dei dettagli del trimestre.

**Schema nome periodo**

**Numerato per anno**

Questa opzione consente di impostare l'etichetta del periodo in base alla sua posizione nell'anno. L'etichetta del periodo è una combinazione del prefisso e del numero del periodo. I numeri di periodo non vengono reimpostati in ciascun trimestre. Ad esempio, se il prefisso del periodo è "P", l'etichetta del sesto periodo sarà P6. Per personalizzare il `Prefisso periodo`, vedere `Prefisso periodo` a pagina 72. Per impostazione predefinita, il numero di ciascun periodo è impostato in base al relativo ordine logico (ad esempio il primo periodo è etichettato come "1"), ma è possibile personalizzarlo selezionando un valore diverso dall'elenco a discesa dei dettagli del periodo.

**Numerato per trimestre**

Questa opzione consente di impostare l'etichetta del periodo in base alla sua posizione nel trimestre. L'etichetta del periodo è una combinazione del prefisso e del numero del periodo. I numeri di periodo vengono reimpostati in ciascun trimestre. Ad esempio, se il prefisso del periodo è "P" e il sesto periodo è il secondo periodo del secondo trimestre, la relativa etichetta sarà P2. Per personalizzare il prefisso del periodo, vedere `Prefisso periodo` a pagina 72. Per impostazione predefinita, il numero di ciascun periodo è impostato in base al relativo ordine logico all'interno del trimestre (ad esempio il primo periodo in un trimestre è etichettato come "1"), ma è possibile personalizzarlo selezionando un valore diverso dall'elenco a discesa dei dettagli del periodo.

**Nomi mese standard**

Questa opzione consente di impostare l'etichetta del periodo sul nome del mese in cui inizia il periodo. Ad esempio, se un periodo è iniziato il 12 di ottobre e termina il 10 di novembre, l'etichetta del periodo sarà Ottobre.

**Nomi periodo personalizzati**

Questa opzione consente di impostare l'etichetta del periodo su qualsiasi stringa. L'etichetta del periodo viene impostata sulla stringa selezionata da `Nome periodo`. Per impostazione predefinita l'ordine dei nomi dei periodi è identico all'ordine dell'elenco di selezione, ma è possibile personalizzarlo selezionando un valore diverso dall'elenco a discesa dei dettagli del periodo.

## Elenchi di selezione degli anni fiscali

Rivedere questi elenchi di selezione personalizzati per personalizzare le etichette dei propri anni fiscali personalizzati.

**`Prefisso trimestre`**

L'elenco di selezione dei prefissi trimestre è un elenco di opzioni del testo che precede il numero o il nome del trimestre se il proprio anno fiscale utilizza lo schema di denominazione dei trimestri **Numerato per anno**. Ad esempio, se il trimestre fiscale è chiamato "T4", "T" sarà il prefisso del trimestre.

**`Prefisso periodo`**

L'elenco di selezione dei prefissi periodo è un elenco di opzioni del testo che precede il numero o il nome del periodo se il proprio anno fiscale utilizza lo schema di denominazione dei periodi **Numerato per anno**. Ad esempio, se il trimestre fiscale è chiamato "P4", "P" sarà il prefisso del periodo.

**`Nome trimestre`**

L'elenco di selezione dei nomi trimestre è un elenco di opzioni dei nomi dei trimestri se il proprio anno fiscale utilizza lo schema di denominazione dei trimestri **Nomi trimestre personalizzati**. Ad esempio, se si desidera assegnare un nome ai trimestri in base alle stagioni (Primavera, Estate, Autunno e Inverno), è possibile impostare l'elenco dei nomi su tali valori.

**`Nome periodo`**

L'elenco di selezione dei nomi periodo è un elenco di opzioni dei nomi dei periodi se il proprio anno fiscale utilizza lo schema di denominazione dei periodi **Nomi periodo personalizzati**. Simile all'elenco di selezione dei nomi trimestre, è possibile scegliere dei nomi significativi per l'elenco di selezione dei nomi periodo.

## Personalizzazione dei nomi degli anni fiscali

Per personalizzare uno di questi elenchi di selezione:

1. Da Imposta, immettere *`Anno fiscale`* nella casella `Ricerca veloce`, quindi selezionare **Anno fiscale**.
2. Fare clic su **Modifica** accanto all'elenco di selezione appropriato.

VEDERE ANCHE:

Informazioni sugli anni fiscali

## Selezione di un modello di anno fiscale personalizzato

Quando si definisce un nuovo anno fiscale personalizzato, è necessario per prima cosa scegliere un modello di anno fiscale personalizzato. Tali modelli consentono una più facile definizione dell'anno fiscale personalizzato, poiché creano un anno fiscale personalizzato semplice che è poi possibile personalizzare in base alle proprie esigenze.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni tranne **Database.com** Edition.

AUTORIZZAZIONI UTENTE

Per modificare il proprio anno fiscale:

- "Personalizza applicazione"

Nota: se si sceglie un modello e ci si accorge in seguito che non è il modello più indicato per la definizione del proprio anno fiscale, è possibile reimpostarlo in qualsiasi momento utilizzando l'opzione **Ripristina struttura dell'anno fiscale**.

Scegliere uno dei tre tipi di modelli:

**4 trimestri in un anno, 13 settimane in un trimestre**

Scegliere uno di questi modelli per il proprio anno fiscale se si desidera che ciascun trimestre presenti lo stesso numero di settimane per trimestre. Tali modelli presentano tutti 4 trimestri, 12 periodi e 52 settimane in un anno. Ogni trimestre è lungo 13 settimane e include tre periodi. Due dei periodi di ciascun trimestre hanno 4 settimane, mentre un periodo ne ha 5. In un modello 4-4-5, ad esempio, il primo e il secondo periodo di un trimestre durano 4 settimane, mentre il terzo ne dura 5. Le settimane sono sempre di 7 giorni. Una tipica personalizzazione di questi modelli è l'aggiunta di settimane extra negli anni bisestili.

**4-4-5**

In ogni trimestre, il periodo 1 ha 4 settimane, il periodo 2 ha 4 settimane e il periodo 3 ha 5 settimane

**4-5-4**

In ogni trimestre, il periodo 1 ha 4 settimane, il periodo 2 ha 5 settimane e il periodo 3 ha 4 settimane

**5-4-4**

In ogni trimestre, il periodo 1 ha 5 settimane, il periodo 2 ha 4 settimane e il periodo 3 ha 4 settimane

**13 periodi in un anno, 4 settimane in un periodo**

Scegliere uno di questi modelli se il proprio anno fiscale è composto da più di 12 periodi e se un trimestre è più lungo degli altri trimestri. Tutti questi modelli presentano 4 trimestri in un anno, 13 periodi all'anno, 3 o 4 periodi per trimestre, 53 settimane in un anno e 4 settimane per periodo (5 settimane nel periodo finale). Le settimane sono generalmente di 7 giorni, ma sarà presente una settimana più corta alla fine dell'anno. La personalizzazione più comune per questo tipo di modello è la creazione o modifica della durata di una settimana corta.

**3-3-3-4**

Il trimestre 1 ha 3 periodi, il trimestre 2 ha 3 periodi, il trimestre 3 ha 3 periodi e il trimestre 4 ha 4 periodi

**3-3-4-3**

Il trimestre 1 ha 3 periodi, il trimestre 2 ha 3 periodi, il trimestre 3 ha 4 periodi e il trimestre 4 ha 3 periodi

**3-4-3-3**

Il trimestre 1 ha 3 periodi, il trimestre 2 ha 4 periodi, il trimestre 3 ha 3 periodi e il trimestre 4 ha 3 periodi

**4-3-3-3**

Il trimestre 1 ha 4 periodi, il trimestre 2 ha 3 periodi, il trimestre 3 ha 3 periodi e il trimestre 4 ha 3 periodi

**Calendario gregoriano**

12 mesi/anno, calendario gregoriano standard.

A differenza degli altri stili di modelli, non è possibile eseguire la personalizzazione avanzata di un anno fiscale che è stato creato da un modello di calendario gregoriano. Utilizzare questo modello solo se si desidera creare un anno fiscale che segua il calendario gregoriano. Tale modello imita le funzionalità degli anni fiscali standard.

VEDERE ANCHE:

Informazioni sugli anni fiscali

## Definizione di un anno fiscale personalizzato

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition.

AUTORIZZAZIONI UTENTE

Per visualizzare l'anno fiscale:

- "Visualizza impostazione e configurazione"

Per modificare il proprio anno fiscale:

- "Personalizza applicazione"

Prima di definire un anno fiscale personalizzato, abilitare gli anni fiscali personalizzati per la propria organizzazione. Per ulteriori informazioni, vedere Abilitazione degli anni fiscali personalizzati a pagina 69.

Abilitare gli anni fiscali personalizzati non significa definirli automaticamente. È necessario definire tutti gli anni fiscali personalizzati della propria società in modo da adattarli al calendario della società stessa.

Se è stato definito un anno fiscale personalizzato e si desidera modificarlo, è possibile modificare la definizione esistente di anno fiscale. Gli anni fiscali personalizzati non possono essere eliminati. Anziché eliminare un anno fiscale esistente, modificarlo finché non soddisfa le proprie esigenze.

Prima di definire o modificare qualsiasi anno fiscale personalizzato, ponderare le eventuali conseguenze sulle previsioni, i rapporti e qualsiasi altro oggetto rivedendo la sezione Informazioni sugli anni fiscali a pagina 66.

### Definizione di un nuovo anno fiscale personalizzato

Per definire un nuovo anno fiscale personalizzato:

1. Da Imposta, immettere *Anno fiscale* nella casella `Ricerca veloce`, quindi selezionare **Anno fiscale**.
2. Fare clic su **Nuovo**. Viene visualizzata la finestra del modello Anno fiscale personalizzato.
3. Scegliere un modello e fare clic su **Continua** per chiudere la finestra di dialogo del modello Anno fiscale personalizzato. Per ulteriori informazioni sui modelli, vedere Selezione di un modello di anno fiscale personalizzato a pagina 73.
4. Impostare la data iniziale e il nome dell'anno fiscale e scegliere il giorno di inizio settimana. È inoltre possibile aggiungere una descrizione dell'anno fiscale.

   Nota: se si tratta del primo anno fiscale personalizzato che è stato definito, i valori `Data di inizio anno fiscale` e `Giorno di inizio settimana` sono impostati sulla data e sul giorno di inizio settimana odierni. Se, invece, è già stato definito un anno fiscale personalizzato, tali valori verranno impostati sul giorno successivo alla data finale degli anni fiscali personalizzati.

   Se si desidera apportare modifiche diverse dalla data iniziale, nome dell'anno o giorno di inizio settimana, vedere Personalizzazione della struttura dell'anno fiscale a pagina 69.
5. In alternativa, rivedere la definizione di anno fiscale facendo clic su **Anteprima**.

   Se è corretta, chiudere l'anteprima e fare clic su **Salva** per salvare il proprio anno fiscale, oppure su **Salva e Nuovo** per salvare il proprio anno fiscale e definirne un altro.

## Modifica di un anno fiscale personalizzato

Per modificare una definizione di anno fiscale personalizzato esistente:

1. Da Imposta, immettere *Anno fiscale* nella casella Ricerca veloce, quindi selezionare **Anno fiscale**.
2. Fare clic sul nome di un anno fiscale definito per rivedere i relativi dettagli. Chiudere l'anteprima dell'anno fiscale per continuare.
3. Fare clic su **Modifica** per l'anno fiscale che si desidera modificare.
4. Modificare i valori Data di inizio anno fiscale, Nome dell'anno fiscale, Descrizione o Data di inizio settimana.

   Se la modifica del valore Data di inizio anno fiscale provoca la sovrapposizione di questo anno fiscale con quello precedente o crea un'interruzione tra anni fiscali, la data finale dell'anno fiscale precedente verrà cambiata al giorno precedente l'inizio di questo anno fiscale.

   Se la modifica della data finale provoca una sovrapposizione di questo anno fiscale con l'anno fiscale successivo o crea un'interruzione tra anni fiscali, la data di inizio dell'anno fiscale successivo verrà impostata sul giorno successivo alla fine di questo anno fiscale.

   Nota: non è possibile modificare la data iniziale o finale di un anno fiscale che ne provoca la sovrapposizione con un anno fiscale definito mediante un modello di anno gregoriano.

   Avvertenza: se si modifica la data iniziale o finale di un qualsiasi trimestre, periodo o settimana, tutti i dati relativi alle previsioni (tra cui quote, cronologia previsioni e Ignora previsione) che rientrano in quell'intervallo di date e tutte le previsioni per gli intervalli di date regolati automaticamente come conseguenza della modifica, andranno persi. Questo vale anche per le modifiche alla data iniziale o finale derivanti dall'aggiunta o eliminazione di periodi.

5. Fare clic su **Anteprima**.
6. Rivedere la definizione dell'anno fiscale. Se è corretta, chiudere l'anteprima e fare clic su **Salva** per salvare l'anno fiscale. Per modifiche più dettagliate, vedere Personalizzazione della struttura dell'anno fiscale a pagina 69.

   Nota: le etichette dei periodi dell'anno fiscale per le previsioni e i rapporti sono impostate dai valori delle etichette predefiniti per i periodi dell'anno fiscale a meno che non le si specifichi. Per modificarle, vedere Personalizzazione delle etichette dell'anno fiscale a pagina 71.

# Impostazione della funzione di ricerca

## Personalizzazione delle impostazioni di ricerca

Per modificare le impostazioni di ricerca dell'organizzazione:

1. Da Imposta, immettere *Impostazioni ricerca* nella casella Ricerca veloce, quindi selezionare **Impostazioni ricerca**.
2. Modificare le impostazioni di ricerca della propria organizzazione.
3. Fare clic su **Salva**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni di ricerca:

- "Personalizza applicazione"

### Impostazioni ricerca

Le impostazioni di ricerca sono le seguenti:

**Abilita elenco a discesa per ricerca dall'intestazione laterale**

L'elenco a discesa per la ricerca dall'intestazione laterale consente di limitare per oggetto le ricerche da parte degli utenti. Se si seleziona Abilita elenco a discesa per ricerca dall'intestazione laterale, nella sezione di ricerca compare un elenco a discesa. Da questo elenco gli utenti possono decidere se effettuare ricerche all'interno di tag, di un oggetto specifico o di tutti gli oggetti.

**Abilita casella di ricerca "Limita ai record di cui sono titolare"**

La casella di controllo Limita ai record di cui sono titolare consente agli utenti di includere solo i record dei quali sono titolari quando immettono delle query di ricerca nell'intestazione laterale.

Nota: la casella di controllo Limita ai record di cui sono titolare visualizzata nella ricerca avanzata è sempre disponibile per tutti gli utenti, indipendentemente da questa impostazione.

**Abilita ricerca contenuto documenti**

Abilitando Abilita ricerca contenuto documenti, è possibile effettuare una ricerca completa dei documenti. Quando viene caricato un nuovo documento o ne viene sostituito uno obsoleto, i relativi contenuti sono disponibili come termini di ricerca per recuperare il documento in questione.

**Abilita ottimizzazione ricerca se il contenuto è principalmente in giapponese, cinese o coreano**

Selezionando la casella di controllo, vengono ottimizzate le ricerche in giapponese, cinese e coreano. Influisce sulla ricerca dall'intestazione laterale e sulla ricerca di account per **Trova duplicati** su un record del lead nella ricerca dall'intestazione laterale e nella ricerca globale. Abilitare l'opzione se le ricerche degli utenti riguardano principalmente giapponese, cinese o coreano e se il testo presente nei campi all'interno dei quali è possibile effettuare ricerche è in larga misura in tali lingue.

Non selezionare l'opzione se si prevede che contenuto e ricerche saranno principalmente in altre lingue.

**Utilizza record utente visualizzati di recente per ricerche vuote e di completamento automatico**

Se l'impostazione è abilitata, l'elenco di record restituito dalla ricerca di completamento automatico e dalla ricerca vuota di un utente viene ricavato dagli ultimi record utente visualizzati dall'utente stesso. Questa impostazione è valida solo per le ricerche di oggetti utente e non per le ricerche di altri oggetti.

Se, invece, l'impostazione non è abilitata, nella finestra di dialogo viene visualizzato un elenco degli ultimi record utente a cui è stato effettuato l'accesso in tutta l'organizzazione.

**Abilita Correzione ortografia solo inglese per la ricerca Knowledge (Beta)**

Se questa impostazione è abilitata, la ricerca suggerisce e cerca ortografie alternative per i termini di ricerca in lingua inglese:

- Nelle schede Articoli e Gestione articoli
- Nello strumento Articoli in Feed caso

- Nell'intestazione laterale Salesforce Knowledge nella Salesforce Console

Questa impostazione si applica alle ricerche di articoli mediante l'API ma non alle ricerche di articoli nella ricerca globale.

**Abilita completamento automatico ricerca dall'intestazione laterale**

Se questa impostazione è abilitata, quando gli utenti iniziano a digitare i termini di ricerca, la ricerca dall'intestazione laterale visualizza un elenco corrispondente di record visualizzati di recente.

Nota: La Ricerca globale include la funzione di completamento automatico e non richiede l'impostazione di una ricerca.

**Abilita scelta rapida risultato ricerca singola**

Se questa impostazione è abilitata, gli utenti saltano la pagina dei risultati della ricerca e vanno direttamente alla pagina dei dettagli del record quando la ricerca restituisce una sola voce.

Questa impostazione non si applica a tag, commenti ai casi (nella ricerca avanzata) e alla ricerca globale. Se il risultato della ricerca è un singolo tag, commento a un caso o elemento nella ricerca globale, viene ancora visualizzata la pagina dei risultati della ricerca.

**Numero di risultati di ricerca visualizzati per oggetto**

L'area Numero di risultati di ricerca visualizzati per oggetto consente di configurare il numero degli elementi che vengono restituiti, per ogni oggetto, nella pagina dei risultati della ricerca. L'impostazione corrente è racchiusa tra parentesi accanto ai singoli oggetti. Per cambiare questa impostazione, selezionare uno o più oggetti, immettere il numero dei risultati per pagina e fare clic su **Salva**. Il nuovo valore deve essere compreso tra 5 e 50.

**Impostazioni di ricerca**

L'area Impostazioni di ricerca consente di abilitare le ricerche ottimizzate e il completamento automatico della ricerca per le ricerche di account, referenti, utenti e qualsiasi oggetto personalizzato.

VEDERE ANCHE:

Linee guida per velocizzare la ricerca

## Personalizzazione dei filtri per i risultati di ricerca degli utenti

1. Nell'elenco correlato di un oggetto nella pagina Risultati di ricerca, fare clic su **Personalizza...** > **Filtri per tutti gli utenti**.

   In alternativa, dalle impostazioni di gestione di un oggetto, accedere a Layout di ricerca e fare clic su **Modifica** accanto a **Campi filtro di ricerca**.

2. Per scegliere le colonne, utilizzare **Aggiungi** e **Rimuovi**.
3. Per riordinare le colonne, utilizzare **Su** e **Giù**.
4. Fare clic su **Salva**.

Nota: I filtri dei risultati di ricerca definiti per un oggetto nell'organizzazione interna sono validi anche per i risultati delle ricerche relativi a quell'oggetto nelle comunità.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

AUTORIZZAZIONI UTENTE

Per modificare i layout di ricerca:

- "Personalizza applicazione"

# Configurazione della ricerca dalla finestra di dialogo Ricerca

È possibile personalizzare quali colonne appaiono agli utenti nei risultati delle ricerche.

EDIZIONI

Disponibile in: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

IN QUESTA SEZIONE:



## Configurazione della finestra di dialogo Ricerca in Salesforce Classic

Abilitare le ricerche ottimizzate e il completamento automatico delle ricerche e personalizzare i campi dei filtri di ricerca.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

Gli amministratori possono configurare le ricerche nei seguenti modi:

- Abilitando le ricerche ottimizzate
- Specificando campi di filtro delle ricerche
- Abilitando il completamento automatico della ricerca

### Abilitazione delle ricerche ottimizzate

Abilitare le ricerche ottimizzate in modo che gli utenti possano utilizzare i caratteri jolly nelle loro ricerche e possano ordinare, filtrare e scorrere le pagine dei risultati. Le ricerche ottimizzate sono supportate per account, referenti, utenti, opportunità e oggetti personalizzati.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

AUTORIZZAZIONI UTENTE

Per abilitare le ricerche ottimizzate:

- "Personalizza applicazione"

Nota: i record degli oggetti personalizzati sono ricercabili nell'interfaccia utente Salesforce solo se l'oggetto personalizzato è associato a una scheda personalizzata. Non è necessario che gli utenti aggiungano la scheda per la visualizzazione.

1. Da Imposta, immettere *`Impostazioni ricerca`* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni ricerca**.
2. Nell'area Impostazioni di ricerca, selezionare gli oggetti per cui si desidera abilitare la funzionalità delle ricerche ottimizzate. Attualmente, questa funzione può essere utilizzata solo per le ricerche di account, referenti, utenti e oggetti personalizzati.
3. Fare clic su **Salva**.

Dopo aver abilitato le ricerche ottimizzate, specificare i campi utilizzabili dagli utenti per filtrare i risultati della ricerca. Se non viene specificato alcun campo, gli utenti non potranno utilizzare i filtri nelle finestre di dialogo di ricerca ottimizzata. I campi configurati per utilizzare le ricerche ottimizzate non supportano la ricerca di singoli caratteri (tranne per le ricerche in cinese, giapponese, coreano e tailandese) o i caratteri jolly all'inizio della stringa di ricerca.

Nota: se si abilitano le ricerche ottimizzate nella propria organizzazione, questa funzione viene abilitata anche per le eventuali pagine Visualforce che vengono create.

VEDERE ANCHE:

Configurazione della finestra di dialogo Ricerca in Salesforce Classic

## Specifica di campi di filtro delle ricerche

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

AUTORIZZAZIONI UTENTE

Per specificare campi di filtro delle ricerche:

- "Personalizza applicazione"

Dopo aver abilitato le ricerche ottimizzate, specificare i campi utilizzabili dagli utenti per filtrare i risultati della ricerca. Se non viene specificato alcun campo, gli utenti non potranno utilizzare i filtri nelle finestre di dialogo di ricerca ottimizzata.

1. Accedere a Layout di ricerca dalle impostazioni di gestione degli account, dei referenti, delle opportunità, degli utenti o degli oggetti personalizzati.
2. Per il layout Campi filtro di ricerca, fare clic su **Modifica**.
3. Utilizzare le frecce per aggiungere o rimuovere i campi dal layout e definire l'ordine in cui devono essere visualizzati i campi. All'elenco Campi selezionati possono essere aggiunti un massimo di sei campi filtro. Per selezionare più di un campo, utilizzare CTRL+clic o MAIUSC+clic per selezionare più elementi in una serie.
4. Fare clic su **Salva**.

VEDERE ANCHE:

Configurazione della finestra di dialogo Ricerca in Salesforce Classic

## Abilitazione del completamento automatico della ricerca

Con il completamento automatico della ricerca, durante la modifica di un campo di ricerca gli utenti possono selezionare gli elementi da un elenco dinamico di record corrispondenti utilizzati di recente. La funzione è supportata per la ricerca di account, referenti, utenti, opportunità e oggetti personalizzati.

1. Da Imposta, immettere *Impostazioni ricerca* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni ricerca**.
2. Nell'area Impostazioni di ricerca, selezionare le ricerche di oggetti per cui si desidera abilitare il completamento automatico. Attualmente, questa funzione può essere utilizzata solo per le ricerche di account, referenti, opportunità, utenti e oggetti personalizzati.
3. Fare clic su **Salva**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

AUTORIZZAZIONI UTENTE

Per abilitare il completamento automatico della ricerca:

- "Personalizza applicazione"

Per utilizzare il completamento automatico della ricerca:

- "Modifica" per il record che comprende il campo di ricerca

VEDERE ANCHE:

Configurazione della finestra di dialogo Ricerca in Salesforce Classic

## Configurazione della ricerca nella finestra di dialogo Ricerca in Lightning Experience

Con l'impostazione di personalizzazione del layout di ricerca Risultati di ricerca, è possibile personalizzare quali colonne far apparire agli utenti nei risultati di ricerca della finestra di dialogo di ricerca. Gli utenti non possono utilizzare queste colonne per ordinare e filtrare. Tali colonne sono progettate per fornire un aiuto contestuale per determinare quale record associare.

Utilizzare **Risultati di ricerca** sotto la personalizzazione **Layout di ricerca** per modificare quali campi visualizzare nei risultati della ricerca sia per la ricerca globale sia per la ricerca dalla finestra di dialogo di ricerca. Non è necessario aggiornare separatamente le **Finestre di dialogo di ricerca**.

L'ordine dei campi nel layout di ricerca incide anche sul campo secondario visualizzato nei risultati istantanei. Il secondo campo utilizzabile, scelto in questa fase, appare come campo secondario nei risultati istantanei. Gli esempi di campi non utilizzabili sono campi con formattazione HTML, campi di immagini in linea o campi di testo lungo.

EDIZIONI

Disponibile nelle versioni: Lightning Experience

Disponibile in: **tutte** le versioni, eccetto **Personal Edition, Contact Manager Edition, Corporate Social Network Edition**

AUTORIZZAZIONI UTENTE

Per specificare campi di filtro delle ricerche:

- "Personalizza applicazione"

## Linee guida per velocizzare la ricerca

EDIZIONI

Disponibile in: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

Seguire queste linee guida per aiutare i propri utenti a trovare le informazioni in modo più rapido.

I record sono inclusi nei risultati della ricerca solo se il campo dell'oggetto che contiene le informazioni corrispondenti al termine di ricerca è ricercabile.

Dopo la creazione o l'aggiornamento del record di un oggetto ricercabile, potrebbero trascorrere circa 15 minuti o più prima che il testo aggiornato diventi ricercabile.

Per velocizzare le ricerche nella propria organizzazione:

**Disabilitare la ricerca per gli oggetti personalizzati nei quali i propri utenti eseguono raramente delle ricerche.**

Scegliere quali oggetti personalizzati possono essere cercati dai propri utenti abilitando l'impostazione **Consenti ricerca** sulla pagina di impostazione dell'oggetto personalizzato.Se non si necessita che i record di un oggetto personalizzato siano ricercabili, disabilitare la ricerca per quell'oggetto personalizzato.Rendere un oggetto personalizzato ricercabile anche quando i propri utenti non hanno bisogno di cercare i record di tale oggetto contribuisce a rallentare le ricerche in tutta l'organizzazione.

Per impostazione predefinita, la ricerca è disabilitata per i nuovi oggetti personalizzati.

Nota: I record degli oggetti personalizzati sono ricercabili nell'interfaccia utente Salesforce solo se l'oggetto personalizzato è associato a una scheda personalizzata. Non è necessario che gli utenti aggiungano la scheda per la visualizzazione.

**Evitare di apportare modifiche significative alla propria organizzazione in una volta sola**

La creazione o l'aggiornamento di molti record contemporaneamente, ad esempio tramite Data Loader, aumenta il tempo necessario a far sì che ciascun record diventi ricercabile. Se la propria organizzazione è molto grande e ha numerosi utenti che apportano aggiornamenti simultanei di frequente, pianificare i caricamenti in blocco e i processi in background in modo che vengano eseguiti negli orari di attività meno intensa.

# Elenchi di selezione Provincia e Paese

## Elenchi di selezione Provincia e Paese

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni tranne Database.com Edition

Gli elenchi di selezione provincia e paese consentono agli utenti di selezionare province e paesi da elenchi predefiniti e standardizzati, invece di immettere i dati relativi a province e paesi nei campi di testo. Gli elenchi di selezione Provincia e Paese consentono una più semplice e rapida immissione dei dati. Contribuiscono a garantire dati più puliti che possono essere utilizzati per altri fini, ad esempio nei rapporti e nei cruscotti digitali. Proteggono l'integrità dei dati impedendo refusi, ortografie alternative e dati indesiderati, anche nei record aggiornati tramite l'API. Le province e i paesi negli elenchi di selezione si basano sui valori ISO-3166 standard, il che li rende compatibili con altre applicazioni.

Gli elenchi di selezione di province e paesi sono disponibili nei campi di indirizzo spedizioni, fatturazione, indirizzo postale e "altro" negli oggetti standard account, referente, contratto, lead, account personali, preventivi e contratti di servizio. Gli elenchi di selezione sono inoltre disponibili per la gestione di utenti e società in Impostazione dell'amministrazione. Per utilizzare l'elenco di selezione, innanzitutto scegliere il paese, quindi scegliere tra le opzioni che compilano automaticamente l'elenco di selezione delle province.

È possibile utilizzare gli elenchi di selezione di province e paesi nella maggior parte dei posti in cui sono disponibili i campi di provincia e paese in Salesforce, tra cui:

- Pagine di modifica e dei dettagli dei record
- Visualizzazioni elenco, rapporti e cruscotti digitali

- Filtri, funzioni, regole e assegnazioni

È inoltre possibile effettuare ricerche negli elenchi di selezione di province e paesi, che sono inoltre supportati nell'Area di lavoro traduzione.

## Limitazioni degli elenchi di selezione di province e paesi

Per impostazione predefinita, gli elenchi di selezione Provincia e Paese includono 239 paesi. Includono anche gli stati e le province di Stati Uniti, Canada, Australia, Brasile, Cina, India, Irlanda, Italia e Messico. Gli elenchi di selezione Provincia e Paese contenenti oltre 1.000 province o paesi possono peggiorare le prestazioni. Gli elenchi di selezione provincia e paese non funzionano con:

- Salesforce a Salesforce
- Salesforce Classic mobile
- Connect Offline
- Visual Workflow o serie di modifiche
- Indici personalizzati o messaggi in uscita

Se l'organizzazione utilizza Data.com, i record Data.com possono contenere province e paesi che non sono inclusi negli elenchi di selezione di province e paesi standard. È necessario aggiungere tali province e paesi all'elenco di selezione affinché gli utenti di Data.com possano aggiungere o pulire questi record. Le province e i paesi che è necessario aggiungere all'elenco di selezione, se utilizzati dall'organizzazione, sono:

- Samoa Americane (AS)
- Guam (GU)
- Hong Kong (HK)
- Isole Marshall (MH)
- Antille Olandesi (AN)
- Isole Mariana Settentrionali (MP)
- Serbia e Montenegro (CS)
- Isole minori esterne degli Stati Uniti (UM)

Nei rapporti sui campi provincia e paese vengono visualizzate le etichette degli elenchi di selezione e non i valori dei codici. Per visualizzare le abbreviazioni dei valori di codice in tutti i punti in cui gli utenti visualizzano nomi di province o paesi, modificare manualmente le etichette Nome provincia o Nome paese impostandole sui valori di codice (per istruzioni sulla modifica, vedere Configurazione degli elenchi di selezione Provincia e Paese a pagina 84). È possibile accedere ai valori di codice di provincia e paese mediante i campi `StateCode` e `CountryCode` in Area di lavoro traduzione o Data Loader.

## Implementazione di Elenchi di selezione Provincia e Paese

Il processo di transizione dai campi di province e paesi basati su testo agli elenchi di selezione di province e paesi si articola in cinque fasi.

1. Configurare i valori di provincia e paese da rendere disponibili nella propria organizzazione.

   Questa operazione è vivamente consigliata poiché consente di personalizzare i valori di provincia e paese e assicura che i dati di provincia e paese continuino a funzionare con qualsiasi sistema di terze parti integrato con Salesforce.

2. Analizzare i dati e le personalizzazioni dell'organizzazione per capire in che modo saranno influenzati dalla conversione.

   Convertire i dati e aggiornare le personalizzazioni, quali le visualizzazioni elenco, i rapporti e le regole di flusso di lavoro, in modo che continuino a funzionare con il nuovo tipo di campi.

3. Convertire i dati esistenti.

La procedura di conversione consente di mappare i diversi valori dell'organizzazione ai valori di elenchi di selezione standard. Ad esempio, si supponga di voler mappare U.S., USA e Stati Uniti a US.

4. Attivare gli elenchi di selezione per gli utenti.

   Se si attivano gli elenchi di selezione provincia e paese senza configurare i valori, analizzare l'organizzazione e convertire i dati esistenti, gli utenti possono utilizzare gli elenchi di selezione nei nuovi record. Tuttavia, tutti i dati esistenti sono incompatibili con il nuovo formato, il che potrebbe compromettere la coerenza e l'integrità dei dati tra i due formati di campo.

5. Se si desidera, analizzare nuovamente e correggere le personalizzazioni o i record che sono stati creati o modificati dopo la prima analisi.

Per una guida con procedure dettagliate per l'implementazione degli elenchi di selezione di province e paesi, vedere Implementazione degli elenchi di selezione di province e paesi.

## Valori di integrazione per gli elenchi di selezione Provincia e Paese

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni tranne Database.com Edition

Un valore di integrazione è un valore di testo personalizzabile collegato a un codice provincia o paese. I valori di integrazione per le province e i paesi standard vengono impostati automaticamente sui nomi completi ISO standard di provincia e paese. I valori di integrazione funzionano in modo analogo ai nomi API di campi e oggetti personalizzati. La configurazione dei valori di integrazione consente integrazioni che vengono impostate prima di abilitare gli elenchi di selezione Provincia e Paese per continuare a funzionare.

Quando si abilitano gli elenchi di selezione Provincia e Paese, i campi `Stato/Provincia` e `Paese` di tipo testo vengono riconvertiti e diventano campi `Valore di integrazione`. Nei rapporti e nelle visualizzazioni elenco, i campi `Valore di integrazione` sono denominati `Stato/Provincia (solo testo)` e `Paese (solo testo)`. Inoltre, per ogni singolo campo `Stato/Provincia (solo testo)` e `Paese (solo testo)`, viene creato un campo `Codice provincia` o `Codice paese` di tipo elenco di selezione. I valori degli elenchi di selezione Provincia e Paese impostati nell'organizzazione determinano i valori disponibili in tali campi codice.

Tra i campi disponibili in ogni valore dell'elenco di selezione Provincia o Paese vi sono `Attivo`, `Visibile`, `Nome`, `Codice` e `Valore di integrazione`. Tutti gli elenchi di selezione Provincia e Paese (per `Indirizzo fatturazione`, `Indirizzo spedizione` e così via) possono accedere ai valori degli elenchi di selezione Provincia e Paese creati dall'utente. L'archiviazione di un codice provincia o paese consente ai record di accedere ad altre informazioni sulle province e i paesi.

Per impostazione predefinita, i campi `Nome` e `Valore di integrazione` per le province e i paesi contengono valori identici. Il valore nel campo `Nome` viene visualizzato dagli utenti che interagiscono con l'elenco di selezione. Il `Valore di integrazione` viene utilizzato da:

- Classi e trigger Apex
- Pagine Visualforce
- Query SOQL
- Query e integrazioni API
- Regole di assegnazione, risposta automatica, convalida e inoltro al livello superiore
- Regole di flusso di lavoro
- Modelli di email
- Pulsanti e link personalizzati
- Personalizzazioni di insiemi di campi
- Rapporti e visualizzazioni elenco

Quando si aggiorna un valore di codice su un record, la colonna `Stato/Provincia (solo testo)` o `Paese (solo testo)` di quel record viene compilata con il valore di integrazione corrispondente. Analogamente, quando si aggiorna la colonna `(solo testo)` di una provincia o di un paese con un valore di integrazione valido, viene mantenuta la sincronia con la colonna del codice della provincia o del paese corrispondente. È possibile modificare i valori di integrazione della propria organizzazione dopo aver abilitato gli elenchi di selezione Provincia e Paese. Tuttavia, quando si aggiornano i valori di integrazione di provincia e paese degli elenchi di selezione, i valori di integrazione sui record non vengono aggiornati. I valori dei nomi non vengono memorizzati sui record. Vengono invece recuperati da Salesforce in base al valore `Codice provincia` o `Codice paese` di un record. Se le province o i paesi negli elenchi di selezione hanno valori di campo diversi per `Nome` e `Valore di integrazione`, assicurarsi che i propri filtri di rapporti o visualizzazioni elenco utilizzino i valori corretti. Utilizzare i nomi nei filtri `Provincia` e `Paese` e utilizzare i valori di integrazione nei filtri `Stato (solo testo)` e `Paese (solo testo)`. In caso contrario, i rapporti potrebbero non riuscire ad acquisire tutti i record pertinenti.

Modificare i propri valori di integrazione in Imposta o utilizzando l'API dei metadati. I campi `Nome` di province e paesi possono essere modificati solo da Imposta. Nell'API dei metadati, i campi `Nome` e `Valore di integrazione` sono denominati rispettivamente `label` e `integrationValue`.

VEDERE ANCHE:

Elenchi di selezione Provincia e Paese

Modifica dei dettagli di province e paesi

Logica di sincronizzazione dei campi degli elenchi di selezione Provincia e Paese

Messaggi di errore degli elenchi di selezione Provincia e Paese

## Configurazione degli elenchi di selezione Provincia e Paese

La configurazione degli elenchi di selezione provincia e paese comporta la scelta di quali stati e paesi si desidera rendere disponibili nella propria organizzazione Salesforce. Consente di rendere disponibili gli elenchi di selezione provincia e paese per finalità quali importazione di dati, utilizzo con sistemi esterni e disponibilità nell'API dei metadati. La configurazione degli elenchi di selezione non è richiesta per abilitare effettivamente gli elenchi di selezione provincia e paese per gli utenti, ma è raccomandata. La configurazione degli elenchi di selezione aiuta ad assicurare la continuità e l'integrità dei dati con i dati e le personalizzazioni di province e paesi esistenti.

Durante la configurazione di province e paesi, iniziare con i paesi e procedere ai relativi stati o province. Per impostazione predefinita, gli elenchi di selezione Provincia e Paese includono 239 paesi. Includono anche gli stati e le province di Stati Uniti, Canada, Australia, Brasile, Cina, India, Irlanda, Italia e Messico. Gli elenchi di selezione Provincia e Paese contenenti oltre 1.000 province o paesi possono peggiorare le prestazioni. Per l'elenco completo dei paesi predefiniti, vedere Paesi standard per gli elenchi di selezione indirizzo.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **tutte** le versioni tranne Database.com Edition

AUTORIZZAZIONI UTENTE

Per configurare gli elenchi di selezione provincia e paese:

- "Modifica tutti i dati"

Nota:

- I valori di integrazione per gli elenchi di selezione provincia e paese possono anche essere configurati tramite l'API dei metadati. Per ulteriori informazioni, vedere la sezione dedicata al componente AddressSettings in *Metadata API Developer's Guide*.
- Gli elenchi di selezione di province e paesi non sono supportati nelle serie di modifiche o nei pacchetti Salesforce. Tuttavia, è possibile spostare le modifiche ai valori di integrazione degli elenchi di selezione provincia e paese tra le organizzazioni Sandbox e di produzione utilizzando l'API dei metadati. Innanzitutto, configurare i propri elenchi di selezione Provincia e Paese nell'organizzazione Sandbox. Quindi, utilizzare l'API dei

metadati per recuperare le configurazioni Sandbox e distribuirle alla propria organizzazione di produzione.

1. Da Imposta, immettere `Elenchi di selezione Provincia e Paese` nella casella `Ricerca veloce`, quindi selezionare **Elenchi di selezione Provincia e Paese**.
2. Nella pagina di impostazione Elenchi di selezione Provincia e Paese, fare clic su **Configura le province e i paesi**.
3. Selezionare dalle opzioni seguenti:

   **`Attivo`**
   Rende il paese disponibile nell'API dei metadati in modo che sia possibile importare record che contengono il paese. Tuttavia, il paese non è disponibile agli utenti in Salesforce finché non viene impostato come visibile.

   **`Visibile`**
   Rende disponibile il paese agli utenti in Salesforce. Prima di poter rendere visibile un paese, è necessario che sia attivo.

4. Fare clic su **Modifica** per visualizzare e modificare i dettagli del paese, inclusa la configurazione dei suoi stati o province.
5. (Facoltativo) In Impostazioni elenco di selezione, selezionare un `Paese predefinito`. Il Paese predefinito compila automaticamente gli elenchi di selezione del paese per i nuovi record dell'organizzazione, ma gli utenti possono selezionare un paese diverso. I paesi predefiniti devono essere sia attivi che visibili.
6. Fare clic su **Salva** per salvare la configurazione.

Nota: le province e i paesi attivi non contrassegnati `Visibile` sono comunque valori validi per la ricerca con filtri. È possibile utilizzare province e paesi invisibili durante la creazione dei filtri in rapporti, visualizzazioni elenco, flussi di lavoro e così via.

VEDERE ANCHE:

Modifica dei dettagli di province e paesi

Elenchi di selezione Provincia e Paese

Valori di integrazione per gli elenchi di selezione Provincia e Paese

## Paesi standard per gli elenchi di selezione indirizzo

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni tranne Database.com Edition

### Paesi standard

Salesforce fornisce i seguenti 239 paesi come standard per gli elenchi di selezione del paese. Un asterisco (*) indica che per quel paese sono disponibili stati o province.

| Codice ISO | Paese |
|---|---|
| AD | Andorra |
| AE | Emirati Arabi Uniti |
| AF | Afghanistan |
| AG | Antigua e Barbuda |
| AI | Anguilla |
| AL | Albania |
| AM | Armenia |

| Codice ISO | Paese |
|---|---|
| AO | Angola |
| AQ | Antartide |
| AR | Argentina |
| AT | Austria |
| AU | Australia* |
| AW | Aruba |
| AX | Isole Aland |
| AZ | Azerbaijan |
| BA | Bosnia ed Erzegovina |
| BB | Barbados |
| BD | Bangladesh |
| BE | Belgio |
| BF | Burkina Faso |
| BG | Bulgaria |
| BH | Bahrain |
| BI | Burundi |
| BJ | Benin |
| BL | Saint Barthélemy |
| BM | Bermuda |
| BN | Brunei Darussalam |
| BO | Bolivia, Stato plurinazionale della |
| BQ | Bonaire, Sint Eustatius e Saba |
| BR | Brasile* |
| BS | Bahamas |
| BT | Bhutan |
| BV | Isola Bouvet |
| BW | Botswana |
| BY | Bielorussia |
| BZ | Belize |
| CA | Canada* |

| Codice ISO | Paese |
| --- | --- |
| CC | Isole Cocos (Keeling) |
| CD | Congo, Repubblica Democratica del |
| CF | Repubblica Centrafricana |
| CG | Congo |
| CH | Svizzera |
| CI | Costa d'Avorio |
| CK | Isole Cook |
| CL | Cile |
| CM | Camerun |
| CN | Cina* |
| CO | Colombia |
| CR | Costa Rica |
| CU | Cuba |
| CV | Capo Verde |
| CW | Curaçao |
| CX | Isola Christmas |
| CY | Cipro |
| CZ | Repubblica Ceca |
| DE | Germania |
| DJ | Gibuti |
| DK | Danimarca |
| DM | Dominica |
| DO | Repubblica Dominicana |
| DZ | Algeria |
| EC | Ecuador |
| EE | Estonia |
| EG | Egitto |
| EH | Sahara Occidentale |
| ER | Eritrea |
| ES | Spagna |

| Codice ISO | Paese |
|---|---|
| ET | Etiopia |
| FI | Finlandia |
| FJ | Fiji |
| FK | Isole Falkland (Malvine) |
| FO | Isole Faroe |
| FR | Francia |
| GA | Gabon |
| GB | Regno Unito |
| GD | Grenada |
| GE | Georgia |
| GF | Guiana francese |
| GG | Guernsey |
| GH | Ghana |
| GI | Gibilterra |
| GL | Groenlandia |
| GM | Gambia |
| GN | Guinea |
| GP | Guadalupa |
| GQ | Guinea Equatoriale |
| GR | Grecia |
| GS | Georgia del Sud e Isole Sandwich meridionali |
| GT | Guatemala |
| GW | Guinea Bissau |
| GY | Guyana |
| HM | Isole Heard e McDonald |
| HN | Honduras |
| HR | Croazia |
| HT | Haiti |
| HU | Ungheria |
| ID | Indonesia |

| Codice ISO | Paese |
|---|---|
| IE | Irlanda* |
| IL | Israele |
| IM | Isola di Man |
| IN | India* |
| IO | Territorio Britannico dell'Oceano Indiano |
| IQ | Iraq |
| IR | Iran, Repubblica Islamica dell' |
| IS | Islanda |
| IT | Italia* |
| JE | Jersey |
| JM | Giamaica |
| JO | Giordania |
| JP | Giappone |
| KE | Kenya |
| KG | Kyrgyzstan |
| KH | Cambogia |
| KI | Kiribati |
| KM | Comore |
| KN | Saint Kitts e Nevis |
| KP | Corea, Repubblica Democratica Popolare di |
| KR | Corea, Repubblica di |
| KW | Kuwait |
| KY | Isole Cayman |
| KZ | Kazakhstan |
| LA | Repubblica Democratica Popolare del Laos |
| LB | Libano |
| LC | Santa Lucia |
| LI | Liechtenstein |
| LK | Sri Lanka |
| LR | Liberia |

| Codice ISO | Paese |
|---|---|
| LS | Lesotho |
| LT | Lituania |
| LU | Lussemburgo |
| LV | Lettonia |
| LY | Jamahiriya Araba Libica |
| MA | Marocco |
| MC | Monaco |
| MD | Moldavia, Repubblica di |
| ME | Montenegro |
| MF | Saint Martin (parte francese) |
| MG | Madagascar |
| MK | Macedonia, ex Repubblica Jugoslava di |
| ML | Mali |
| MM | Myanmar |
| MN | Mongolia |
| MO | Macao |
| MQ | Martinica |
| MR | Mauritania |
| MS | Montserrat |
| MT | Malta |
| MU | Mauritius |
| MV | Maldive |
| MW | Malawi |
| MX | Messico* |
| MY | Malesia |
| MZ | Mozambico |
| NA | Namibia |
| NC | Nuova Caledonia |
| NE | Niger |
| NF | Isola Norfolk |

| Codice ISO | Paese |
| --- | --- |
| NG | Nigeria |
| NI | Nicaragua |
| NL | Olanda |
| NO | Norvegia |
| NP | Nepal |
| NR | Nauru |
| NU | Niue |
| NZ | Nuova Zelanda |
| OM | Oman |
| PA | Panama |
| PE | Perù |
| PF | Polinesia Francese |
| PG | Papua Nuova Guinea |
| PH | Filippine |
| PK | Pakistan |
| PL | Polonia |
| PM | Saint Pierre e Miquelon |
| PN | Pitcairn |
| PS | Palestina |
| PT | Portogallo |
| PY | Paraguay |
| QA | Qatar |
| RE | Riunione |
| RO | Romania |
| RS | Serbia |
| RU | Federazione Russa |
| RW | Rwanda |
| SA | Arabia Saudita |
| SB | Isole Salomone |
| SC | Seychelles |

| Codice ISO | Paese |
| --- | --- |
| SD | Sudan |
| SE | Svezia |
| SG | Singapore |
| SH | Sant'Elena, Ascensione e Tristan da Cunha |
| SI | Slovenia |
| SJ | Svalbard e Jan Mayen |
| SK | Slovacchia |
| SL | Sierra Leone |
| SM | San Marino |
| SN | Senegal |
| SO | Somalia |
| SR | Suriname |
| SS | Sudan del Sud |
| ST | Sao Tome e Principe |
| SV | El Salvador |
| SX | Sint Maarten (parte olandese) |
| SY | Repubblica Araba di Siria |
| SZ | Swaziland |
| TC | Isole Turks e Caicos |
| TD | Ciad |
| TF | Territori Francesi Meridionali |
| TG | Togo |
| TH | Thailandia |
| TJ | Tajikistan |
| TK | Tokelau |
| TL | Timor-Est |
| TM | Turkmenistan |
| TN | Tunisia |
| TO | Tonga |
| TR | Turchia |

| Codice ISO | Paese |
|---|---|
| TT | Trinidad e Tobago |
| TV | Tuvalu |
| TW | Taiwan |
| TZ | Tanzania, Repubblica Unita di |
| UA | Ucraina |
| UG | Uganda |
| US | Stati Uniti* |
| UY | Uruguay |
| UZ | Uzbekistan |
| VA | Santa Sede (Stato della Città del Vaticano) |
| VC | San Vincenzo e Grenadine |
| VE | Venezuela, Repubblica Bolivariana del |
| VG | Isole Vergini, Britanniche |
| VN | Vietnam |
| VU | Vanuatu |
| WF | Wallis e Futuna |
| WS | Samoa |
| YE | Yemen |
| YT | Mayotte |
| ZA | Sud Africa |
| ZM | Zambia |
| ZW | Zimbabwe |

## Modifica dei dettagli di province e paesi

È possibile aggiungere province e paesi alla propria organizzazione, oppure modificare i valori di province e paesi esistenti, nella pagina dei dettagli di una provincia o di un paese. Per aggiungere o modificare uno stato o una provincia, accedere alla relativa pagina dei dettagli tramite la pagina dei dettagli del paese associato.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **tutte** le versioni tranne Database.com Edition

AUTORIZZAZIONI UTENTE

Per aggiungere o modificare i dettagli di province e paesi:
- "Modifica tutti i dati"

1. Da Imposta, immettere *Provincia* nella casella Ricerca veloce, quindi selezionare **Elenchi di selezione Provincia e Paese**.
2. Fare clic su **Configura le province e i paesi**.
3. Fare clic su **Nuovo paese** per aggiungere un paese, oppure fare clic su **Modifica** per un paese elencato.
4. Specificare le opzioni desiderate in Informazioni sul paese.

**Nome del paese**

Per impostazione predefinita, il nome ISO standard. Questo è il nome visualizzato dagli utenti nell'interfaccia utente Salesforce.

**Codice paese**

Per impostazione predefinita, il codice ISO standard a due lettere. Se si modifica un codice ISO, il nuovo valore deve essere univoco. I codici non fanno distinzione tra maiuscole e minuscole e possono contenere solo caratteri ASCII e numeri. Non è possibile modificare i codici ISO standard di province e paesi. È possibile modificare i codici paese di province e paesi personalizzati solo prima di abilitare tali province e paesi per i propri utenti.

**Valore di integrazione**

Valore di testo personalizzabile collegato a un codice provincia o paese. I valori di integrazione per le province e i paesi standard vengono impostati automaticamente sui nomi completi ISO standard di provincia e paese. I valori di integrazione funzionano in modo analogo ai nomi API di campi e oggetti personalizzati. La configurazione dei valori di integrazione consente integrazioni che vengono impostate prima di abilitare gli elenchi di selezione Provincia e Paese per continuare a funzionare.

È possibile modificare i valori di integrazione per farli corrispondere ai valori utilizzati in altre aree dell'organizzazione. Si supponga ad esempio di disporre di una regola di flusso di lavoro che come nome del paese utilizza USA anziché il valore predefinito Stati Uniti. Se si imposta manualmente il valore di integrazione per il codice paese US su *USA*, la regola di flusso di lavoro non si interrompe quando si abilitano gli elenchi di selezione Provincia e Paese.

Quando si aggiorna un valore di codice su un record, la colonna Stato/Provincia (solo testo) o Paese (solo testo) di quel record viene compilata con il valore di integrazione corrispondente. Analogamente, quando si aggiorna la colonna (solo testo) di una provincia o di un paese con un valore di integrazione valido, viene mantenuta la sincronia con la colonna del codice della provincia o del paese corrispondente. È possibile modificare i valori di integrazione della propria organizzazione dopo aver abilitato gli elenchi di selezione Provincia e Paese. Tuttavia, quando si aggiornano i valori di integrazione di provincia e paese degli elenchi di selezione, i valori di integrazione sui record non vengono aggiornati. I valori dei nomi non vengono memorizzati sui record. Vengono invece recuperati da Salesforce in base al valore Codice provincia o Codice paese di un record. Se le province o i paesi negli elenchi di selezione hanno valori di campo diversi per Nome e Valore di integrazione, assicurarsi che i propri filtri di rapporti o visualizzazioni elenco utilizzino i valori corretti. Utilizzare i nomi nei filtri Provincia e Paese e utilizzare i valori di integrazione nei filtri Stato (solo testo) e Paese (solo testo). In caso contrario, i rapporti potrebbero non riuscire ad acquisire tutti i record pertinenti.

**Attivo**

Rende il paese disponibile nell'API dei metadati in modo che sia possibile importare record che contengono il paese. Tuttavia, il paese non è disponibile agli utenti in Salesforce finché non viene impostato come visibile.

**`Visibile`**
Rende disponibile il paese agli utenti in Salesforce. Per poter rendere visibile un paese, è necessario che sia attivo.

5. Se si sta aggiungendo un paese, fare clic su **Aggiungi**.
6. Se si sta modificando un paese, specificare l'opzione per le province:

**`Attivo`**
Rende la provincia disponibile nell'API dei metadati in modo che sia possibile importare record che contengono la provincia. Tuttavia, la provincia non è disponibile agli utenti in Salesforce finché non viene impostata come visibile.

**`Visibile`**
Rende disponibile la provincia agli utenti in Salesforce. Per poter rendere visibile una provincia, è necessario che sia attiva.

7. Fare clic su una delle seguenti opzioni, se lo si desidera.
   - **Nuova provincia** per aggiungere uno stato o una provincia personalizzati. Nella pagina Nuova provincia, specificare un `Nome della provincia`, un `Codice provincia`, un `Valore di integrazione` e selezionare se la nuova provincia è `Attiva` o `Visibile`. Per salvare la nuova provincia, fare clic su **Aggiungi**.
   - **Modifica** per visualizzare e modificare i dettagli dello stato o della provincia, inclusi `Nome della provincia`, `Codice provincia` e `Valore di integrazione`.
8. Fare clic su **Salva**.

VEDERE ANCHE:

Configurazione degli elenchi di selezione Provincia e Paese

Elenchi di selezione Provincia e Paese

Valori di integrazione per gli elenchi di selezione Provincia e Paese

Elenchi di selezione Provincia e Paese e API dei metadati

## Elenchi di selezione Provincia e Paese e API dei metadati

In caso di modifica di numerosi valori di integrazione degli elenchi di selezione Provincia e Paese, l'utilizzo dell'API dei metadati è un metodo più efficiente della modifica dei valori in Imposta.

È possibile utilizzare l'API dei metadati per modificare i paesi e le province presenti negli elenchi di selezione Provincia e Paese. Non è possibile utilizzare l'API dei metadati per creare o eliminare nuovi paesi o province. Innanzitutto, configurare i propri elenchi di selezione Provincia e Paese nell'organizzazione Sandbox. Quindi, utilizzare l'API dei metadati per recuperare le configurazioni Sandbox e distribuirle alla propria organizzazione di produzione. Per informazioni sull'utilizzo degli elenchi di selezione Provincia e Paese nell'API dei metadati, cercare "AddressSettings" nel manuale *Metadata API Developer's Guide*.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni tranne Database.com Edition

VEDERE ANCHE:

Valori di integrazione per gli elenchi di selezione Provincia e Paese

Modifica dei dettagli di province e paesi

## Preparazione all'analisi dei dati di province e paesi e personalizzazioni

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni tranne Database.com Edition

Prima di effettuare la transizione dai campi di province e paesi basati su testo agli elenchi di selezione di province e paesi standardizzati, analizzare l'organizzazione per capire in che modo verrà influenzata dalla modifica. Questo processo di scoperta mostra all'utente le aree e le modalità in cui i dati di province e paesi appaiono nell'organizzazione e i casi in cui vengono usati nelle personalizzazioni, ad esempio le visualizzazioni elenco e i rapporti. Dopo avere analizzato i risultati dell'analisi, sarà possibile pianificare la conversione dei dati, l'aggiornamento delle personalizzazioni e l'attivazione degli elenchi di selezione province e paesi.

Questo processo è diverso per ogni organizzazione. Per alcune, la transizione dai campi di testo di province e paesi a elenchi di selezione standardizzati è semplice e gestibile. Tuttavia, se nell'organizzazione sono diffusamente utilizzati i metadati di province e paesi, il processo potrebbe essere lungo e complesso. Salesforce consiglia di effettuare l'analisi dell'organizzazione per tempo e di frequente in modo da poter effettuare una transizione senza problemi ai nuovi elenchi. Tenere presenti le seguenti procedure consigliate e considerazioni.

- L'analisi non converte i dati né corregge le personalizzazioni. Convertire i dati separatamente e aggiornare individualmente le personalizzazioni.
- È possibile continuare a lavorare normalmente nella propria organizzazione durante l'analisi.
- La procedura di analisi consente di identificare i pacchetti gestiti interessati ma non fornisce un meccanismo per risolvere i problemi legati ai pacchetti.
- L'analisi non identifica le formule che includono metadati di province e paesi.
- Non è possibile utilizzare valori di visualizzazione nelle regole di convalida o nelle regole di flusso di lavoro che utilizzano funzioni di formula di confronto. Se le regole di convalida o di flusso di lavoro nei campi provincia o paese utilizzano `BEGINS`, `CONTAINS`, `ISCHANGED` o `REGEX`, utilizzare `ISPICKVAL` con i valori di codice di provincia e paese nelle funzioni di confronto.
- L'analisi non identifica le visualizzazioni elenco personali e i rapporti che utilizzano metadati di province e paesi. I singoli utenti devono aggiornare autonomamente quelle personalizzazioni.
- I lead convertiti non vengono analizzati. I valori di provincia e paese non vengono aggiornati sui record dei lead convertiti quando si abilitano gli elenchi di selezione provincia e paese.
- Analizzare più volte la propria organizzazione: dopo avere aggiornato una personalizzazione, effettuare nuovamente l'analisi per assicurarsi che le modifiche abbiano risolto i problemi esistenti senza crearne di nuovi.

VEDERE ANCHE:

Analisi dei dati di province e paesi e personalizzazioni

Elenchi di selezione Provincia e Paese

## Analisi dei dati di province e paesi e personalizzazioni

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni tranne Database.com Edition

AUTORIZZAZIONI UTENTE

Per analizzare i dati di province e paesi e le personalizzazioni:

- "Modifica tutti i dati"

  E

  "Crea documenti"

La ricerca dei valori di province e paesi basati su testo in un'organizzazione identifica i luoghi e i modi in cui i dati di province e paesi basati su testo appaiono nei record esistenti. Ad esempio, è possibile visualizzare tutti i modi in cui "Stati Uniti" è stato salvato come valore di testo, quali U.S.A., USA, America, Estados Unidos e persino le voci contenenti errori ortografici, come Statti Uniti. Inoltre, questa analisi mostra le aree in cui i dati di province e paesi sono utilizzati nelle personalizzazioni, quali:

- Visualizzazioni elenco
- Rapporti
- Regole di convalida
- Pulsanti e link personalizzati
- Regole di flusso di lavoro
- Modelli di email
- Insiemi di campi
- Classi e trigger Apex
- Pagine Visualforce

Al termine dell'analisi, l'utente riceve due messaggi email contenenti i link a rapporti dettagliati: uno relativo ai dati di indirizzo e l'altro alle personalizzazioni. Dopo avere analizzato i rapporti, iniziare l'operazione di conversione dei dati esistenti in valori di elenchi di selezione e l'aggiornamento delle personalizzazioni in modo che funzionino con i nuovi campi di elenchi di selezione.

1. Da Imposta, immettere *Elenchi di selezione Provincia e Paese* nella casella `Ricerca veloce`, quindi selezionare **Elenchi di selezione Provincia e Paese**.
2. Nella pagina di impostazione Elenchi di selezione Provincia e Paese, fare clic su **Analizza ora**, quindi su **Analizza**.

   Data Management > State and Country Picklists

   Scan for Affected Data and Customizations — Help for this Page

   Identify where state and country text data is used in your organization and find customizations that you may need to update when you switch to picklists.

   1. Click Scan. You'll receive two emails when the scan is complete: one regarding affected address data and one regarding affected customizations.
   2. Click the links in the emails to see how your data and customizations are affected.

   Scan (Last scan completed: 10/24/2012 9:25 AM)

3. Attendere un messaggio email contenente i risultati.

   A seconda delle dimensioni e della complessità dell'organizzazione, la generazione dei risultati può richiedere da pochi minuti a qualche ora.

   Nota: Le email vengono inviate dall'indirizzo noreply@salesforce.com. La riga dell'oggetto sarà "Analisi dei dati degli indirizzi Salesforce" o "Analisi delle personalizzazioni degli indirizzi Salesforce". Se non si ricevono le email, verificare che non siano state bloccate da un filtro antispam.

4. Fare clic sul link presente in ciascuna email per visualizzare un documento contenente il rapporto relativo ai dati o alle personalizzazioni interessati.
5. Nella pagina dei dettagli Documento, fare clic su **Visualizza file**.

Document
AddressDiscovery_2012-08-13 1047.txt
Help for this Page

Document Detail — Edit Properties | Delete | Replace Document | Email Document

| | |
|---|---|
| Document Name | AddressDiscovery_2012-08-13 1047.txt |
| Document Unique Name | AddressDiscovery_2012_08_13_1047_txt |
| Internal Use Only | |
| Document Content Searchable | ✓ |
| Folder | My Personal Documents |
| Author | Admin User [Change] |
| File Extension | txt |
| MIME Type | text/plain |
| Size | 1015 bytes |
| Description | |
| Keywords | |
| | View file |
| Created By | Admin User, 8/13/2012 10:47 AM — Modified By: Admin User, 8/13/2012 10:47 AM |

Edit Properties | Delete | Replace Document | Email Document

VEDERE ANCHE:

Elenchi di selezione Provincia e Paese

## Preparazione alla conversione dei dati di province e paesi

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni tranne Database.com Edition

Se l'organizzazione Salesforce include valori di province e paesi basati su testo, è possibile convertire tali dati in valori di elenchi di selezione standardizzati. La conversione dei dati esistenti consente di continuare a lavorare con i dati dopo che si è passati agli elenchi di selezione. Si supponga, ad esempio, di avere un rapporto che raccoglie tutti i lead degli agenti di vendita nello stato di Washington e che il rapporto sia generato mediante il valore elenco di selezione provincia Washington. Per fare in modo che tutti i record con i valori di provincia basati su testo, quali Wash., WA e Washington vengano inclusi nel rapporto, convertire i dati relativi alla provincia basati su testo in valori di elenchi di selezione standardizzati.

La conversione dei dati di testo esistenti su province e paesi in valori di elenchi di selezione standardizzati aiuta ad assicurare l'integrità dei dati una volta abilitati gli elenchi di selezione nella propria organizzazione. Al salvataggio di record contenenti valori di province e paesi non presenti negli elenchi di selezione, gli utenti visualizzano degli errori di convalida. Inoltre, i rapporti diventano inaffidabili quando i record creati prima dell'abilitazione degli elenchi di selezione Provincia e Paese contengono valori di province e paesi diversi dai record utilizzati durante la creazione degli elenchi di selezione.

Durante la conversione dei dati, Salesforce inizia dai paesi, quindi passa alle province. Vi sono alcuni fattori da ricordare nel corso del processo di conversione:

- Salvare spesso. È possibile uscire dallo strumento di conversione e ritornarvi in qualsiasi momento.
- È possibile continuare a lavorare normalmente nella propria organizzazione durante la conversione dei dati.
- Non è possibile effettuare la conversione dei dati durante l'analisi dei dati e delle personalizzazioni interessati o durante la distribuzione degli elenchi di selezione di province e paesi.
- Le diverse fasi del processo possono essere ripetute e annullate in qualsiasi momento fino a che gli elenchi di selezione vengono abilitati per gli utenti. Dopo che gli elenchi di selezione sono stati abilitati, non è più possibile annullare la conversione.

- Se si utilizza Pulitura Data.com, è consigliabile sospendere i processi di pulitura finché la conversione non è terminata.

VEDERE ANCHE:

Conversione dei dati di province e paesi

Elenchi di selezione Provincia e Paese

## Conversione dei dati di province e paesi

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni tranne Database.com Edition

AUTORIZZAZIONI UTENTE

Per convertire i dati di province e paesi basati su testo:

- "Modifica tutti i dati"

Prima di convertire i valori di province e paesi nell'impostazione Elenchi di selezione Provincia e Paese, configurare gli elenchi di selezione per la propria organizzazione. In questo modo, quando gli elenchi di selezione vengono abilitati, tutti i record nuovi e aggiornati utilizzeranno il valore di integrazione specificato, contribuendo a garantire la coerenza e la precisione dei dati dell'organizzazione.

Durante la conversione dei dati di province e paesi basati su testo in valori compatibili con gli elenchi di selezione, si scelgono valori di testo specifici e si selezionano i valori standard a cui si desidera mapparli. Ad esempio, è possibile selezionare tutte le occorrenze di "USA" e modificarle in "Stati Uniti".

Convertire prima i paesi, quindi gli stati e le province.

È possibile convertire fino a 2.000 valori di paesi e fino a 2.000 valori di province, ma gli elenchi di selezione contenenti più di 1.000 stati o province possono peggiorare le prestazioni.

1. Da Imposta, immettere `Elenchi di selezione Provincia e Paese` nella casella `Ricerca veloce`, quindi selezionare **Elenchi di selezione Provincia e Paese**.
2. Nella pagina di impostazione Elenchi di selezione Provincia e Paese, fare clic su **Converti ora**. Salesforce apre la pagina Converti paesi, che visualizza tutti i valori di testo dei paesi visualizzati nell'organizzazione e il numero di volte in cui viene utilizzato ogni valore.
3. Selezionare `Cambia` per uno o più valori da convertire. Ad esempio, selezionare `Cambia` per tutte le occorrenze di Stati Uniti.
4. Nella sezione `Cambia in`, scegliere il paese in cui si desidera convertire i valori di testo e fare clic su **Salva nell'elenco modifiche**.

   Nota: Se i paesi o le province vengono mappati a `Valore sconosciuto`, gli utenti visualizzano o paesi e le province nei loro record. Tuttavia, al salvataggio dei record gli utenti visualizzano errori a meno che non trasformino ogni paese o provincia in un valore valido prima del salvataggio.

5. Ripetere i punti 3 e 4 per altri valori di paese, ad esempio per il Canada.
   Salesforce tiene traccia delle modifiche pianificate nell'area Elenco modifiche.
6. Dopo che sono stati mappati tutti i paesi, fare clic su **Avanti** per convertire i valori delle province.

   Nella colonna Paese di origine è possibile identificare il paese associato alla provincia in questione.

7. Nella pagina Conferma modifiche, fare clic su **Fine** per tornare alla pagina di panoramica dell'impostazione oppure su **Concludi e abilita gli elenchi di selezione** per convertire i valori e attivare gli elenchi di selezione di province e paesi nella propria organizzazione.

Considerazioni sull'annullamento:

- Nella pagina Converti paesi o Converti province, fare clic su **Annulla** in qualsiasi momento per ripristinare i valori nell'elenco delle modifiche.
- Nella pagina Converti province, fare clic su **Precedente** per tornare alla pagina Converti paesi e modificare le mappature dei paesi.

- Anche dopo avere selezionato **Fine**, è comunque possibile convertire i valori di province e paesi. Dopo che sono stati abilitati gli elenchi di selezione, tuttavia, non è più possibile modificare le mappature della conversione.

VEDERE ANCHE:

Elenchi di selezione Provincia e Paese

## Abilitazione e disabilitazione degli elenchi di selezione Provincia e Paese

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni tranne Database.com Edition

AUTORIZZAZIONI UTENTE

Per attivare e disattivare gli elenchi di selezione provincia e paese:

- "Modifica tutti i dati"

Quando si abilitano gli elenchi di selezione Provincia e Paese, tali elenchi diventano immediatamente disponibili agli utenti. Tuttavia, la compilazione dei campi dei codici ISO sui record esistenti da parte di Salesforce può richiedere del tempo. Se gli utenti cercano di modificare la provincia o il paese di un record prima che il campo del codice sia stato compilato, viene chiesto di selezionare un valore per il codice.

1. Da Imposta, immettere *Elenchi di selezione Provincia e Paese* nella casella `Ricerca veloce`, quindi selezionare **Elenchi di selezione Provincia e Paese**.
2. Nella pagina di impostazione Elenchi di selezione Provincia e Paese, fare clic su **Abilita** per attivare gli elenchi di selezione.

   Nota:

   - È anche possibile abilitare gli elenchi di selezione provincia e paese al termine della conversione dei dati basati su testo esistenti in valori di elenchi di selezione. Vedere Conversione dei dati di province e paesi.

3. Per disattivare gli elenchi di selezione provincia e paese, fare clic su **Disabilita** nella pagina di impostazione Elenchi di selezione Provincia e Paese.

   Importante: Tenere presente che se si disabilitano gli elenchi di selezione di province e paesi:

   - Per i record che non sono stati salvati dopo l'abilitazione degli elenchi di selezione, i valori di province e paesi tornano ai valori di testo originali.
   - Per i record che sono stati salvati dopo l'abilitazione degli elenchi di selezione, i valori di integrazione di province e paesi sostituiscono i valori di testo originali.
   - I riferimenti agli elenchi di selezione di province e paesi nelle personalizzazioni (ad esempio, aggiornamenti di campo di flusso di lavoro, modelli di email, pagine Visualforce) diventano non validi.
   - Le colonne e i filtri che fanno riferimento ai campi degli elenchi di selezione nei rapporti e nelle visualizzazioni elenco scompaiono.

VEDERE ANCHE:

Elenchi di selezione Provincia e Paese

## Logica di sincronizzazione dei campi degli elenchi di selezione Provincia e Paese

Quando si salvano dei record con valori di elenchi di selezione Provincia e Paese, Salesforce sincronizza i valori di integrazione e dei codici dei record per le province e i paesi. Non è possibile modificare direttamente i valori di integrazione di province o paesi sulle pagine dei dettagli dei record. È possibile modificare direttamente i valori di integrazione di province o paesi dei record solo con flussi di lavoro, Apex Code, integrazioni API e così via.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni tranne Database.com Edition

| Modifica | Risultato |
| --- | --- |
| Aggiornamento del codice provincia o paese di un record con un valore valido. | Salesforce aggiorna il valore di integrazione della provincia o del paese in modo che corrisponda al codice. |
| Aggiornamento di un valore di integrazione provincia o paese di un record con un valore valido. | Salesforce aggiorna il codice provincia o paese del record in modo che corrisponda al valore di integrazione. |
| Rimozione del codice paese di un record, senza però rimuovere il codice provincia corrispondente. | Salesforce rimuove il codice provincia del record e i valori di integrazione del paese e della provincia. |
| Creazione o aggiornamento di un record con valori di provincia e paese. La nuova provincia non si trova nel nuovo paese. | Non viene salvata alcuna modifica. Viene visualizzato un messaggio di errore. |
| Aggiornamento dei valori di integrazione e del codice di provincia o paese in un record esistente. I nuovi valori di integrazione e del codice non corrispondono. | Non viene salvata alcuna modifica. Viene visualizzato un messaggio di errore. |
| Creazione di un record in cui i valori di integrazione e del codice provincia o paese non corrispondono. | Salesforce aggiorna il valore di integrazione del nuovo record in modo che corrisponda al valore del codice. |

VEDERE ANCHE:

Elenchi di selezione Provincia e Paese

Valori di integrazione per gli elenchi di selezione Provincia e Paese

Messaggi di errore degli elenchi di selezione Provincia e Paese

# Messaggi di errore degli elenchi di selezione Provincia e Paese

Quando si tenta di salvare record i cui valori di testo per province o paesi non corrispondono, possono verificarsi diversi errori. Le seguenti informazioni chiariscono tali messaggi di errore.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni tranne Database.com Edition

| Errore | Causa |
| --- | --- |
| Paese non valido specificato per il campo | Il codice paese non corrisponde ad alcun paese esistente. |
| Si è verificato un problema con questo paese, anche se può sembrare corretto. Selezionare un paese dall'elenco dei paesi validi. | Il valore di integrazione del paese non corrisponde ad alcun paese esistente. Oppure, il valore del paese è stato mappato su `Valore sconosciuto` durante una conversione di dati. |
| Valore di integrazione e codice ISO per il campo non corrispondenti | Il codice e i valori di integrazione corrispondono a province o paesi diversi. |
| È necessario specificare un paese prima di specificare il valore di una provincia per il campo | Il record dispone di un codice provincia o di un valore di integrazione ma non di un codice paese. Non è possibile salvare una provincia senza un paese corrispondente. |
| Il paese esistente non riconosce il valore della provincia per il campo | Il codice provincia e i valori di integrazione appartengono a una provincia di un paese diverso. |
| Provincia non valida specificata per il campo | Il codice provincia non corrisponde ad alcuna provincia esistente. |

VEDERE ANCHE:

Elenchi di selezione Provincia e Paese

Valori di integrazione per gli elenchi di selezione Provincia e Paese

Logica di sincronizzazione dei campi degli elenchi di selezione Provincia e Paese

# Personalizzazione delle impostazioni dell'interfaccia utente

1. Da Imposta, immettere *Interfaccia utente* nella casella Ricerca veloce, quindi selezionare **Interfaccia utente**.
2. Selezionare o deselezionare ogni casella di controllo per modificare le impostazioni per l'organizzazione.
3. Salvare le modifiche.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Le impostazioni dell'interfaccia utente disponibili variano a seconda della versione di Salesforce utilizzata.

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni dell'interfaccia utente:

- "Personalizza applicazione"

## Impostazioni dell'interfaccia utente

**Abilita sezioni comprimibili**

Consentono all'utente di comprimere o espandere sezioni nelle pagine dei dettagli dei record utilizzando la freccia accanto all'intestazione della sezione. Se si abilitano le sezioni comprimibili, assicurarsi che per ogni layout di pagina siano visualizzate le intestazioni di sezione. Le sezioni rimangono espanse o compresse finché l'utente non modifica le impostazioni della scheda. Se l'organizzazione ha abilitato i tipi di record, Salesforce memorizza un'impostazione diversa per ogni tipo di record.

**Mostra Creazione rapida**

La sezione Creazione rapida nella pagina iniziale della scheda consente agli utenti di creare velocemente un nuovo record con pochi dati e viene visualizzata, per impostazione predefinita, sulle pagine iniziali delle schede per i lead, gli account, i referenti, le previsioni e le opportunità. È possibile controllare se l'area Creazione rapida è visualizzata su tutte le pagine iniziali delle schede relative.

Nota: L'impostazione Mostra Creazione rapida influenza anche la possibilità degli utenti di creare nuovi record dalla finestra di dialogo di ricerca. Ad esempio, con l'impostazione abilitata, gli utenti possono creare un nuovo account all'interno della finestra di dialogo di ricerca account durante la creazione o la modifica di un referente. La creazione di nuovi record nella finestra di dialogo di ricerca è possibile solo se è disponibile l'opzione Creazione rapida per il tipo di record scelto. Sebbene venga visualizzata per tutti gli utenti, per utilizzare Creazione rapida, gli utenti devono sempre disporre dell'autorizzazione "Crea" appropriata.

**Abilita dettagli effetto di attivazione**

Quando gli utenti passano con il mouse sopra il link di un record nell'elenco Elementi recenti dell'intestazione laterale o in un campo di ricerca di una pagina dei dettagli del record, nei dettagli dell'effetto di attivazione viene visualizzata una sovrapposizione interattiva contenente informazioni dettagliate su quel record. Gli utenti possono visualizzare rapidamente le informazioni relative a un record prima di selezionare **Visualizza** per la pagina dei dettagli di un record o **Modifica** per la pagina di modifica. I campi visualizzati nei dettagli effetto di attivazione sono determinati dal layout di mini pagina del record. I campi visualizzati nei dettagli effetto di attivazione di un documento non sono personalizzabili. Questa opzione è abilitata per impostazione predefinita.

Nota: per visualizzare i dettagli effetto di attivazione di un record, gli utenti devono disporre dell'accesso di condivisione appropriato a quel record, nonché del livello di protezione a livello di campo necessario per i campi del layout di mini pagina.

**Abilita link effetto di attivazione elenco correlato**

I link effetto di attivazione relativi agli elenchi correlati vengono visualizzati in Imposta nella parte superiore delle pagine dei dettagli dei record e degli oggetti personalizzati. Gli utenti possono passare con il mouse sopra un link effetto di attivazione per visualizzare l'elenco correlato corrispondente e il relativo numero di record in una sovrapposizione interattiva che consente di visualizzare e gestire rapidamente gli elementi dell'elenco correlato. Gli utenti possono inoltre fare clic su un link effetto di attivazione elenco correlato per posizionarsi direttamente sul contenuto dell'elenco correlato senza dover scorrere la pagina. La casella di controllo Abilita link effetto di attivazione elenco correlato è selezionata per impostazione predefinita.

**Abilita caricamento separato degli elenchi correlati**

Abilitando l'opzione, per prima cosa gli utenti vedono i dettagli dei record principali. Mentre vengono caricati i dati degli elenchi correlati, viene visualizzato un indicatore di avanzamento. Il caricamento separato può migliorare le prestazioni nelle pagine dei dettagli dei record per le organizzazioni caratterizzate da quantità elevate di elenchi correlati. Per impostazione predefinita l'opzione è disabilitata. Tenere presente che l'opzione non è valida per le pagine Visualforce, per le pagine utente, per il portale Self-Service, né per altre pagine delle quali non è possibile controllare il layout.

**Abilita modifica in linea**

La modifica in linea consente agli utenti di modificare rapidamente i valori dei campi, direttamente nella pagina dei dettagli di un record. L'opzione è abilitata per impostazione predefinita ed è valida per tutti gli utenti all'interno dell'organizzazione.

Nota: ciò non abilita la modifica in linea per i profili. Selezionare `Abilita visualizzazioni elenco profili ottimizzate` in Imposta.

**Abilita elenchi ottimizzati**

Gli elenchi ottimizzati offrono la possibilità di visualizzare, personalizzare e modificare i dati degli elenchi per velocizzare la produttività giornaliera. Quando viene abilitata con l'impostazione `Abilita modifica in linea`, gli utenti possono anche modificare i record direttamente dall'elenco, senza necessità di allontanarsi dalla pagina. Questa opzione è abilitata per impostazione predefinita.

Nota: ciò non abilita gli elenchi ottimizzati per i profili. Selezionare `Abilita visualizzazioni elenco profili ottimizzate` in Imposta.

**Abilita nuovo tema interfaccia utente**

Nota: A partire dal rilascio Summer '10, nelle nuove organizzazioni il nuovo tema interfaccia utente è abilitato per impostazione predefinita.

Il nuovo tema interfaccia utente aggiorna l'aspetto di Salesforce e sposta i link dell'utente, ad esempio Imposta ed Esci, sotto al nome utente di tutti gli utenti dell'organizzazione. Il nuovo tema interfaccia utente non è supportato nei Portali e nella scheda Console.

Solo gli utenti con i browser supportati possono visualizzare il nuovo tema interfaccia utente.

**Abilita Gestore barra delle schede**

Il Gestore barra delle schede organizza automaticamente le schede nella barra principale delle schede al fine di evitare lo scorrimento orizzontale della pagina. Determina in modo dinamico quante schede possono essere visualizzate in base alla larghezza della finestra del browser e inserisce in un elenco a discesa le schede che si trovano oltre l'area visualizzabile del browser.

Nota: Tenere presenti le seguenti limitazioni:

- Il Gestore barra delle schede non è disponibile con il portale partner o il Portale Clienti.
- Il Gestore barra delle schede è disponibile solo con il nuovo tema dell'interfaccia utente. Le organizzazioni che utilizzano il vecchio tema dell'interfaccia utente possono abilitare la funzione, ma questa non sarà disponibile agli utenti fino a che non viene abilitato anche il nuovo tema.
- Il Gestore barra delle schede non è disponibile su Internet Explorer 6.

**Abilita visualizzazioni elenco in formato stampa**

Le visualizzazioni elenco in formato stampa consentono agli utenti di stampare con facilità le visualizzazioni elenco. Quando questa opzione è abilitata, gli utenti possono fare clic sul link **Formato stampa** da qualsiasi elenco per aprire una nuova finestra del browser, nella quale la visualizzazione elenco corrente sarà visualizzata in un formato semplice e pronto per la stampa. Questo link si trova accanto al link **Guida in linea relativa a questa pagina** nella barra del titolo colorata della pagina.

**Abilita controllo ortografico**

Disponibile in tutte le versioni. Se l'opzione è selezionata, il pulsante **Controlla ortografia** viene visualizzato in determinate aree dell'applicazione in cui viene inserito testo, ad esempio per inviare un messaggio email o per creare eventi, operazioni, casi, note e soluzioni. Facendo clic sul pulsante, viene eseguito il controllo ortografico del testo. Il controllo ortografico non funziona in tutte le

lingue supportate da Salesforce. Ad esempio, il controllo ortografico non supporta il tailandese, il russo e le lingue a due byte come giapponese, coreano e cinese.

**Abilita Controllo ortografico per operazioni ed eventi**

Disponibile in tutte le versioni. Abilita il pulsante **Controlla ortografia** quando gli utenti creano o modificano operazioni o eventi. Il controllo ortografico analizza il campo `Descrizione` negli eventi e il campo `Commenti` nelle operazioni.

**Abilita personalizzazione delle pagine profilo utente Chatter**

Consente agli amministratori di personalizzare le schede della pagina profilo utente Chatter. Ciò include l'aggiunta di schede personalizzate e la rimozione delle schede predefinite. Se l'opzione è disabilitata, gli utenti vedranno solo le schede Feed e Panoramica.

## Impostazioni delle intestazioni laterali

**Abilita intestazione laterale comprimibile**

L'intestazione laterale comprimibile consente agli utenti di visualizzare o nascondere l'intestazione laterale in tutte le pagine che solitamente includono l'intestazione laterale. Se abilitata, l'intestazione laterale comprimibile diventa disponibile a tutti gli utenti dell'organizzazione, ma ogni utente può scegliere la propria opzione di visualizzazione. È possibile scegliere un'intestazione laterale visibile in qualsiasi momento, oppure comprimere l'intestazione per visualizzarla solo quando necessario facendo clic sul bordo dell'intestazione compressa.

Nota: Gli utenti dei call center non vedranno le chiamate in arrivo se l'intestazione laterale viene compressa.

Suggerimento: Se l'organizzazione utilizza le divisioni, si consiglia di mantenere l'intestazione laterale fissa e sempre visibile per poter accedere all'elenco a discesa Divisioni in qualsiasi momento.

**Mostra componenti intestazione laterale personalizzata in tutte le pagine**

Se si dispone di layout di pagina iniziale personalizzati che includono componenti dell'intestazione laterale, questa opzione consente di rendere disponibili tali componenti in tutte le pagine per tutti gli utenti dell'organizzazione. Se si desidera che solo determinati utenti visualizzino i componenti dell'intestazione laterale in tutte le pagine, assegnare a questi utenti l'autorizzazione "Mostra intestazione laterale personalizzata su tutte le pagine".

## Impostazioni del calendario

**Abilita link effetto di attivazione pagina iniziale per gli eventi**

Abilita i link effetto di attivazione nella sezione calendario della scheda Pagina iniziale. Nella scheda Pagina iniziale, passare il mouse sopra l'oggetto di un evento per vederne i dettagli in una sovrapposizione interattiva. Questa opzione è abilitata per impostazione predefinita. Tenere presente che questa casella di controllo si riferisce solo alla scheda Pagina iniziale; i link effetto di attivazione sono sempre disponibili sulle altre visualizzazioni calendario.

I campi disponibili nelle sovrapposizioni dettagli evento e modifica vengono definiti in un layout di mini pagina.

Nota: se si creano eventi intera giornata, si consiglia di aggiungere il campo `Evento intera giornata` al layout di mini pagina.

**Abilita modifica trascinamento della selezione sulle visualizzazioni calendario**

Abilita il trascinamento di eventi sulle visualizzazioni calendario giornaliere e settimanali dei singoli utenti. Ciò consente agli utenti di riprogrammare gli eventi senza uscire dalla pagina. Questa opzione è abilitata per impostazione predefinita.

Nota: Quando è attivata questa casella di controllo, le visualizzazioni calendario potrebbero essere caricate più lentamente.

**Abilita Clic e crea eventi sulle visualizzazioni calendario**

Consente agli utenti di creare eventi sulle visualizzazioni calendario giornaliere e settimanali facendo doppio clic su un orario specifico e immettendo i dettagli dell'evento in una sovrapposizione interattiva. I campi disponibili nelle sovrapposizioni dettagli evento e modifica vengono definiti in un layout di mini pagina.

Tenere presente che gli eventi ricorrenti e gli eventi multiutente non sono supportati per Clic e crea eventi sulle visualizzazioni calendario.

**Abilita pianificazione trascinamento della selezione sulle visualizzazioni elenco**

Consente agli utenti di creare eventi associati a record mediante il trascinamento dei record dalle visualizzazioni elenco alle visualizzazioni settimana del calendario e l'immissione dei dettagli dell'evento in una sovrapposizione interattiva. Per impostazione predefinita l'opzione è disabilitata. I campi disponibili nelle sovrapposizioni dettagli evento e modifica vengono definiti in un layout di mini pagina.

**Abilita link effetto di attivazione per elenco Operazioni personali**

Abilita i link effetto di attivazione per le operazioni nella sezione Operazioni personali della scheda Pagina principale e nella visualizzazione giorno del calendario. Questa opzione è abilitata per impostazione predefinita. Gli utenti possono passare il mouse sull'oggetto di un'operazione per vederne i dettagli in una sovrapposizione interattiva.

Le informazioni presentate su queste sovrapposizioni vengono configurate dall'amministratore.

## Impostazioni del nome

Nota: Le impostazioni del nome possono essere abilitate contattando l'assistenza clienti di Salesforce.

**Abilitazione del secondo nome per i nomi di persona**

Questa opzione consente di visualizzare il campo `Secondo nome` per gli oggetti persona, in modo da poter rappresentare meglio il nome di una persona associata a un record.

**Abilitazione dei suffissi dei nomi per i nomi di persona**

Questa opzione consente di visualizzare il campo `Suffisso` per gli oggetti persona, in modo da poter rappresentare meglio il nome di una persona associata a un record.

## Impostazioni di configurazione

**Abilita Editor layout di pagina ottimizzato**

Quando è abilitato, l'editor di layout di pagina ottimizzato sostituisce l'interfaccia corrente per la modifica dei layout di pagina con un editor WYSIWYG contenente tutte le funzionalità dell'editor di layout di pagina originale oltre a numerose funzioni più avanzate.

**Abilita visualizzazioni elenco profili ottimizzate**

Abilita le visualizzazioni di elenchi ottimizzati e la modifica in linea nella pagina di elenco dei profili. Con la modifica in linea nelle visualizzazioni di elenchi ottimizzati, è possibile gestire più profili contemporaneamente.

**Abilita interfaccia utente profilo ottimizzata**

Abilita l'interfaccia utente profilo ottimizzata, che consente di navigare e cercare fra le impostazioni di un singolo profilo agevolmente, nonché di modificarle.

**Abilita Streaming API**

Abilita Streaming API, che consente di ricevere notifiche, in modo sicuro e scalabile, in caso di modifiche ai dati che soddisfano una query SOQL definita dall'utente. Questo campo è selezionato per impostazione predefinita. Se la casella di controllo non è visibile, verificare innanzitutto che la versione di Salesforce in uso preveda l'accesso all'API. Se la versione di Salesforce in uso prevede l'accesso all'API e la casella di controllo non è visualizzata, rivolgersi a Salesforce.

**Abilita troncamento oggetto personalizzato**

Abilita il troncamento degli oggetti personalizzati, che elimina in modo definitivo tutti i record da un oggetto personalizzato pur mantenendo l'oggetto e i relativi metadati intatti per uso futuro.

**Abilita interfaccia utente Imposta migliorata**

Quando è disabilitata, gli utenti con Salesforce Classic accedono alle loro impostazioni personali dal menu Imposta. Quando è abilitata, gli utenti con Salesforce Classic accedono alle loro impostazioni personali dal menu Impostazioni personali, accessibile dal menu

del nome utente. Inoltre, il link Imposta viene spostato dal menu del nome utente al menu dell'applicazione Force.com. Se si modifica questa impostazione, notificare tutti gli utenti della propria organizzazione.

**Abilita ricerca avanzata in Imposta (beta)**

Se l'opzione è abilitata, gli utenti possono cercare pagine di impostazione, profili personalizzati, insiemi di autorizzazioni, gruppi pubblici, ruoli e utenti dall'intestazione laterale in Imposta. Se è disabilitata, gli utenti possono cercare solo le pagine di Imposta.

Nota:

- la ricerca avanzata in Imposta è in versione beta, la qualità è a livello di produzione ma con alcune limitazioni note.
- Alcuni elementi per i quali si può eseguire la ricerca (come gli insiemi di autorizzazioni) non sono disponibili in alcune versioni. Gli utenti non possono cercare elementi che non sono inclusi nella versione in uso.

## Impostazioni avanzate

**Attiva Stampa unione estesa**

Abilita la Stampa unione estesa per l'organizzazione. Quando la casella di controllo è selezionata, il link **Stampa unione globale** è disponibile nell'area Strumenti delle pagine iniziali di account, referenti e lead. Inoltre, le singole stampe unione richieste dall'elenco correlato Cronologia attività di un record vengono eseguite utilizzando la funzionalità Stampa unione estesa.

Stampa unione estesa è disponibile solo su richiesta. Se si è interessati a questa funzionalità, contattare l'Assistenza clienti di Salesforce.

# Servizi Mappe e Posizione

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**.

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni di mappe e posizione:

- "Personalizza applicazione"

I servizi Mappe e Posizione utilizzano Google Maps per visualizzare le mappe basate sui campi indirizzo standard, abilitare la creazione di mappe Visualforce e consentire agli utenti di immettere nuovi indirizzi con il completamento automatico.

Per generare l'immagine di una mappa, un indirizzo deve contenere i campi via e città e la provincia, il codice postale o il paese. Se il campo di un indirizzo non contiene una delle informazioni richieste, non verrà visualizzata la mappa nella pagina dei dettagli di un record.

L'immagine della mappa sull'indirizzo è statica, ma se si fa clic sull'immagine, Google Maps viene visualizzato in una nuova scheda del browser sul desktop e un'applicazione mappe viene visualizzata su un dispositivo mobile.

Se nell'organizzazione è abilitato l'accesso offline a Salesforce1, quando il dispositivo di un utente è offline non viene visualizzata alcuna mappa.

Per abilitare i servizi mappe e posizione dell'organizzazione:

1. Da Imposta, immettere *Mappe* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di Mappe e Posizione** e fare clic su **Modifica**.
2. Selezionare `Abilita i servizi Mappe e Posizione`.
3. Fare clic su **Salva**.

# Completamento automatico sugli indirizzi standard

È possibile abilitare il completamento automatico negli indirizzi standard per tutti gli utenti di Salesforce1. Questo consente agli utenti di immettere testo nei campi di indirizzo standard e visualizzare i possibili indirizzi corrispondenti in un elenco di selezione.

I risultati degli elenchi di selezione per l'autocompletamento su indirizzi standard sono ottimizzati per questi paesi:

- USA
- Giappone
- Regno Unito
- Canada
- Australia
- Germania
- Francia
- Olanda
- Brasile
- Spagna
- Russia
- Svezia

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**.

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni di mappe e posizione:

- "Personalizza applicazione"

Per abilitare l'autocompletamento nei campi indirizzo standard:

1. Da Imposta, immettere *Mappe* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di Mappe e Posizione** e fare clic su **Modifica**.
2. Selezionare `Abilita l'autocompletamento nei campi indirizzo standard`.
3. Fare clic su **Salva**.

Nota:

- L'autocompletamento dei campi indirizzo standard è disponibile per tutte le versioni di Salesforce1 e per Lightning Experience.

# Personalizzazione di rapporti e cruscotti digitali

Impostare rapporti e cruscotti digitali in modo da fornire le informazioni agli utenti nel modo più adeguato per loro.

Per accedere a questa pagina, da Imposta immettere *Rapporti* nella casella Ricerca veloce, quindi selezionare **Impostazioni rapporti e cruscotti digitali**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni di rapporti e cruscotti digitali:

- "Personalizza applicazione"

IN QUESTA SEZIONE:

Disponibilità di funzioni utili per gli utenti di rapporti e cruscotti digitali

È possibile abilitare o disabilitare diverse funzioni dell'interfaccia utente che possono essere utili per ottimizzare l'uso dei rapporti e dei cruscotti digitali. Si tratta di impostazioni il cui scopo è semplificare la gestione e che non influenzano i dati restituiti dai rapporti e dai cruscotti digitali.

Consentire agli utenti di abbonarsi alle notifiche sui rapporti

Consentire agli utenti di abbonarsi ai rapporti per ricevere notifiche ogni volta che determinate metriche soddisfano le condizioni specificate dagli utenti.

Personalizzazione delle notifiche tramite email per rapporti e cruscotti digitali

Scegliere il modo in cui comunicare agli utenti le modifiche delle informazioni nei rapporti e nei cruscotti digitali in uso.

Impostazione di un tipo di rapporto personalizzato

Un *tipo di rapporto* definisce la serie di record e campi disponibile per un rapporto basato sulle relazioni tra un oggetto principale e gli oggetti ad esso correlati. I rapporti mostrano solo i record che soddisfano i criteri definiti nel tipo di rapporto.

Abilitazione della condivisione ottimizzata per i rapporti e i cruscotti digitali

Quando si abilita la condivisione delle applicazioni analitiche, Salesforce converte i livelli esistenti di accesso alle cartelle degli utenti a nuovi e più dettagliati livelli di accesso.

Configurazione dei rapporti con trend storico

Per mettere a disposizione degli utenti i rapporti con trend storico, configurare mediante dei filtri la quantità di dati che viene acquisita per i rapporti con trend storico. Quindi selezionare i campi necessari per i rapporti storici.

VEDERE ANCHE:

Aggiornamento della creazione guidata rapporto

# Disponibilità di funzioni utili per gli utenti di rapporti e cruscotti digitali

È possibile abilitare o disabilitare diverse funzioni dell'interfaccia utente che possono essere utili per ottimizzare l'uso dei rapporti e dei cruscotti digitali. Si tratta di impostazioni il cui scopo è semplificare la gestione e che non influenzano i dati restituiti dai rapporti e dai cruscotti digitali.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni di rapporti e cruscotti digitali:

- "Personalizza applicazione"

IN QUESTA SEZIONE:



## Abilitazione della visualizzazione delle intestazioni dei rapporti per gli utenti durante lo scorrimento

Le intestazioni di rapporto movibili consentono di mantenere visualizzate le intestazioni di colonna e di riga indipendentemente da quanto gli utenti scorrono i risultati.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni di rapporti e cruscotti digitali:

- "Personalizza applicazione"

Grazie alle intestazioni di rapporto movibili, gli utenti possono scorrere fino in fondo i rapporti molto lunghi senza dovere tornare all'inizio del rapporto per vedere i nomi delle intestazioni delle colonne.

Inoltre, è possibile fare clic sulle intestazioni di rapporti movibili in modo da ordinare i dati di una colonna specifica. Quando l'utente ordina i dati facendo clic sull'intestazione di rapporto movibile, il rapporto si aggiorna e la visualizzazione torna all'inizio dei risultati del rapporto.

Le intestazioni movibili sono disponibili per i rapporti tabulari, di riepilogo e a matrice.

1. Da Imposta, immettere `Rapporti` nella casella `Ricerca veloce`, quindi selezionare **Impostazioni rapporti e cruscotti digitali**.
2. Selezionare o deselezionare **Abilita intestazioni rapporto movibili**.
3. Fare clic su **Salva**.

## Reperimento rapido dei cruscotti digitali per gli utenti

La funzione Trova cruscotti digitali utilizza il completamento automatico per consentire agli utenti di trovare rapidamente i cruscotti nella scheda Cruscotti digitali, immettendo soltanto le prime lettere del nome nel filtro di ricerca.

Tutti i cruscotti digitali che corrispondono al testo immesso vengono visualizzati dinamicamente nell'elenco a discesa. L'elenco visualizza per primi i cruscotti digitali visualizzati di recente; gli altri cruscotti digitali sono invece visualizzati in ordine alfabetico in base alla cartella. I primi 1.000 risultati vengono visualizzati in un unico elenco; in seguito vengono visualizzati 500 risultati per ogni pagina. Gli utenti vedono solo i cruscotti digitali nelle cartelle a cui possono accedere. Disabilitare questa opzione per utilizzare invece l'elenco a discesa statico.

Questa opzione è abilitata per impostazione predefinita.

1. Da Imposta, immettere *Rapporti* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni rapporti e cruscotti digitali**.
2. Selezionare o deselezionare **Abilita Trova cruscotti digitali**.
3. Fare clic su **Salva**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni di rapporti e cruscotti digitali:

- "Personalizza applicazione"

## Abilitazione dell'invio di componenti dei cruscotti digitali in Chatter per gli utenti

Le istantanee dei componenti dei cruscotti digitali consentono agli utenti di inviare immagini statiche dei componenti del cruscotto ai feed Chatter, rendendo le istantanee visibili a tutti gli utenti.

1. Assicurarsi che sia abilitato il tracciamento dei feed Chatter.
2. Da Imposta, immettere *Rapporti* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni rapporti e cruscotti digitali**.
3. Selezionare o deselezionare **Abilita istantanee componenti dei cruscotti digitali**.

Importante: Questa opzione consente agli utenti di ignorare le impostazioni di visibilità del cruscotto digitale e di rendere visibili le istantanee a tutti gli utenti Chatter. Sebbene in questo modo risulti più semplice condividere dati temporali specifici senza dover aggiungere gli utenti nelle cartelle dei cruscotti digitali, è necessario tenere presente che gli utenti potrebbero inviare inavvertitamente dati sensibili o riservati.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni di rapporti e cruscotti digitali:

- "Personalizza applicazione"

## Esclusione dai rapporti della dichiarazione di non responsabilità sulle informazioni riservate

Per impostazione predefinita, i piè di pagina dei rapporti includono una dichiarazione di non responsabilità che recita "Informazioni riservate - Non divulgare". Tale dichiarazione ricorda agli utenti di condividere i rapporti con cautela e consente di assicurarsi che i propri rapporti non siano visualizzati da terzi. È possibile, a propria discrezione, escludere la dichiarazione di non responsabilità dai rapporti.

1. Da Imposta, immettere *Impostazioni rapporti e cruscotti digitali* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni rapporti e cruscotti digitali**.
2. Selezionare **Escludi Dichiarazione di non responsabilità dai rapporti esportati** ed **Escludi Dichiarazione di non responsabilità dalle pagine Esecuzione rapporto e dalle pagine Formato stampa**.
3. Fare clic su **Salva**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **tutte** le versioni tranne **Database.com** Edition

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni di rapporti e cruscotti digitali:
- "Personalizza applicazione"

# Consentire agli utenti di abbonarsi alle notifiche sui rapporti

Consentire agli utenti di abbonarsi ai rapporti per ricevere notifiche ogni volta che determinate metriche soddisfano le condizioni specificate dagli utenti.

1. Da Imposta, immettere *Notifiche rapporto* nella casella `Ricerca veloce`, quindi selezionare **Notifiche rapporto**.
2. Selezionare l'opzione per abilitare le notifiche rapporto.
3. Fare clic su **Salva**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni di rapporti e cruscotti digitali:
- "Personalizza applicazione"

# Personalizzazione delle notifiche tramite email per rapporti e cruscotti digitali

Scegliere il modo in cui comunicare agli utenti le modifiche delle informazioni nei rapporti e nei cruscotti digitali in uso.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni di rapporti e cruscotti digitali:

- "Personalizza applicazione"

1. Da Imposta, immettere *Notifiche per email* nella casella Ricerca veloce, quindi selezionare **Notifiche per email**.
2. Selezionare o deselezionare le seguenti opzioni per modificare le notifiche per l'organizzazione:

   **Consenti invio di rapporti e cruscotti digitali agli utenti del portale**

   Se si abilita questa opzione, tutti gli utenti interni e dei portali specificati come destinatari ricevono rapporti e cruscotti digitali. Se questa opzione non viene abilitata, solo gli utenti interni di Salesforce possono ricevere rapporti e notifiche di aggiornamento dei cruscotti digitali.

   Questa opzione, disabilitata per impostazione predefinita, è disponibile nelle organizzazioni che utilizzano le versioni Enterprise Edition, Unlimited Edition e Performance Edition per cui è impostato un Portale Clienti o un Portale partner.

   **Utilizza immagini compatibili con Lotus Notes nei messaggi email con cruscotti digitali**

   È possibile inviare notifiche di aggiornamento dei cruscotti digitali a utenti specifici al termine dell'aggiornamento pianificato di un cruscotto digitale. Per impostazione predefinita, Salesforce invia le immagini in messaggi email con cruscotti digitali sotto forma di file .png (Portable Network Graphic), che non sono supportati in Lotus Notes. Quando si abilita l'opzione Utilizza immagini compatibili con Lotus Notes nei messaggi email con cruscotti digitali, Salesforce utilizza immagini .jpg, supportate in Lotus Notes, per l'invio di messaggi email con cruscotti digitali. Per visualizzare l'opzione è necessaria l'autorizzazione “Pianifica cruscotti digitali”.

   Nota: i messaggi email con cruscotti digitali che contengono immagini compatibili con Lotus Notes sono significativamente più grandi e la qualità dell'immagine potrebbe essere inferiore.

3. Fare clic su **Salva**.

# Impostazione di un tipo di rapporto personalizzato

Un *tipo di rapporto* definisce la serie di record e campi disponibile per un rapporto basato sulle relazioni tra un oggetto principale e gli oggetti ad esso correlati. I rapporti mostrano solo i record che soddisfano i criteri definiti nel tipo di rapporto.

Ad esempio, un amministratore può creare un tipo di rapporto che mostra solo domande di lavoro con un curriculum associato; le domande senza curriculum non verranno visualizzate nei rapporti che utilizzano questo tipo. Un amministratore può anche mostrare record che *potrebbero* avere record correlati, ad esempio le domande con o senza curriculum. In questo caso, tutte le domande, con o senza curriculum, sono disponibili per i rapporti che utilizzano questo tipo.

è possibile creare tipi di rapporto personalizzati a partire dai quali gli utenti possono eseguire i propri rapporti sui rapporti e sui cruscotti digitali dell'organizzazione. Durante la definizione di un tipo di rapporto personalizzato, selezionare Rapporti o Cruscotti digitali nell'elenco a discesa `Oggetto principale` della pagina Nuovo tipo di rapporto personalizzato.

Suggerimento: Una volta terminata la creazione del tipo di rapporto, valutare come sfruttarlo al meglio:

- Aggiungere il tipo di rapporto personalizzato alle applicazioni che si caricano su Force.com AppExchange.
- Gli utenti designati come traduttori con autorizzazione "Visualizza impostazione e configurazione" possono tradurre i tipi di rapporto personalizzato mediante l'Area di lavoro traduzione.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare o aggiornare tipi di rapporto personalizzato:
- "Gestisci tipi di rapporto personalizzato"

Per eliminare i tipi di rapporto personalizzato:
- "Modifica tutti i dati"

IN QUESTA SEZIONE:

1. Creazione di un tipo di rapporto personalizzato

   Scegliere l'oggetto principale che sarà supportato dal nuovo tipo di rapporto, assegnargli un nome e una descrizione utile. Contrassegnarlo come "in fase di sviluppo" fino a quando si è pronti a renderlo disponibile agli utenti per la generazione di rapporti.

2. Aggiunta di oggetti secondari a un tipo di rapporto personalizzato

   Per consentire ai rapporti di ricavare dati non solo dall'oggetto principale, si possono aggiungere uno o più oggetti correlati a un tipo di rapporto.

3. Definizione del layout dei campi per i rapporti creati a partire da un tipo di rapporto personalizzato

   Dopo avere definito un tipo di rapporto personalizzato e scelto le relative relazioni tra oggetti è possibile specificare i campi standard e personalizzati che possono essere visualizzati in un rapporto se questo viene creato o eseguito a partire da un tipo di rapporto personalizzato.

4. Gestione dei tipi di rapporto personalizzato

   Una volta creato un tipo di rapporto personalizzato è possibile personalizzarlo, modificarlo ed eliminarlo.

5. Limiti dei tipi di rapporto

   I tipi di rapporto personalizzato sono soggetti ad alcuni limiti per garantirne le prestazioni e la fruibilità.

## Creazione di un tipo di rapporto personalizzato

Scegliere l'oggetto principale che sarà supportato dal nuovo tipo di rapporto, assegnargli un nome e una descrizione utile. Contrassegnarlo come "in fase di sviluppo" fino a quando si è pronti a renderlo disponibile agli utenti per la generazione di rapporti.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare o aggiornare tipi di rapporto personalizzato:
- "Gestisci tipi di rapporto personalizzato"

Per eliminare i tipi di rapporto personalizzato:
- "Modifica tutti i dati"

1. Da Imposta, immettere *`Tipi di rapporto`* nella casella `Ricerca veloce`, quindi selezionare **Tipi di rapporto**.
2. Fare clic su **Nuovo tipo di rapporto personalizzato**.
3. Selezionare l'`Oggetto principale` per il tipo di rapporto personalizzato.

   Suggerimento:
   - È possibile scegliere tra tutti gli oggetti, anche quelli che non si è autorizzati a visualizzare. Ciò consente di creare tipi di rapporto per svariati utenti.
   - Una volta salvato un tipo di rapporto, non è possibile modificare l'oggetto principale.
   - Se l'oggetto principale di un tipo di rapporto è un oggetto personalizzato e l'oggetto personalizzato viene eliminato, il tipo di rapporto e tutti i rapporti creati a partire da esso vengono automaticamente eliminati.
   - Se si rimuove un oggetto da un tipo di rapporto, tutti i riferimenti a tale oggetto e agli oggetti associati vengono automaticamente rimossi dai rapporti e dai cruscotti digitali basati su tale tipo.

4. Immettere l'`Etichetta tipo di rapporto` e il `Nome tipo di rapporto`. L'etichetta può contenere al massimo 50 caratteri. Il nome è utilizzato dall'API SOAP.
5. Immettere una descrizione del tipo di rapporto personalizzato, lunga al massimo 255 caratteri.

   Nota: fornire una descrizione significativa in modo tale che gli utenti abbiano un'idea chiara dei dati disponibili per i rapporti. Ad esempio: *`Account con referenti. Rapporto su account e relativi referenti. Gli account senza referenti non sono visualizzati.`*.

6. Selezionare la categoria nella quale memorizzare il tipo di rapporto personalizzato.
7. Selezionare uno `Stato distribuzione`:
   - Scegliere `In fase di sviluppo` durante la progettazione e il test e anche per la modifica. Il tipo di rapporto e i relativi rapporti sono nascosti per tutti gli utenti, tranne quelli con autorizzazione "Gestisci tipi di rapporto personalizzato". Solo gli utenti con tale autorizzazione possono creare ed eseguire i rapporti utilizzando i tipi di rapporto in fase di sviluppo.
   - Scegliere `Distribuito` quando si è pronti per consentire a tutti gli utenti di accedere al tipo di rapporto.

   Nota: Lo `Stato distribuzione` di un tipo di rapporto personalizzato passa da `Distribuito` a `In fase di sviluppo` se il relativo oggetto principale è un oggetto personalizzato il cui `Stato distribuzione` cambia in modo analogo.

8. Fare clic su **Avanti**.

   Nota: uno sviluppatore può modificare un tipo di rapporto personalizzato in un pacchetto gestito dopo il suo rilascio e aggiungervi nuovi campi. Gli abbonati ricevono automaticamente queste modifiche quando installano una nuova versione del pacchetto gestito. Gli sviluppatori non possono tuttavia eliminare oggetti dal tipo di rapporto dopo il rilascio del pacchetto. Se in un tipo di rapporto personalizzato si elimina un campo che fa parte di un pacchetto gestito e che è stato inserito in bucket o utilizzato in raggruppamenti, si riceve un messaggio di errore.

## Aggiunta di oggetti secondari a un tipo di rapporto personalizzato

Per consentire ai rapporti di ricavare dati non solo dall'oggetto principale, si possono aggiungere uno o più oggetti correlati a un tipo di rapporto.

1. Fare clic sulla casella sotto l'oggetto principale.
2. Selezionare un oggetto secondario.

   Vengono visualizzati solo gli oggetti correlati.

   Suggerimento: Digitare testo nella casella di ricerca per trovare rapidamente gli oggetti.

3. Per ogni oggetto secondario, selezionare uno dei seguenti criteri:
   - `Ciascun record "A" deve avere almeno un record "B" correlato.` Solo i record principali con record secondari vengono visualizzati nel rapporto.
   - `I record "A" possono avere o meno record "B" correlati.` I record principali vengono visualizzati indipendentemente dal fatto che abbiano o meno record secondari.

   Se gli utenti sono l'oggetto principale, selezionare gli oggetti secondari in base al campo, ad esempio Account (Titolare account) o Account (Creato da).

4. Aggiungere al massimo tre oggetti secondari.

   Il numero di elementi secondari dipende dagli oggetti scelti.

5. Fare clic su **Salva**.

Esempio:

- Se si sceglie che l'oggetto A potrebbe o non potrebbe avere l'oggetto B, tutti gli oggetti successivi includono automaticamente tale associazione potrebbe-non potrebbe nel tipo di rapporto personalizzato. Ad esempio, se gli account sono l'oggetto primario e i referenti l'oggetto secondario e si sceglie che gli account potrebbero o non potrebbero avere referenti, tutti gli oggetti terziari e quaternari inclusi nel tipo di rapporto personalizzato per impostazione predefinita vengono impostati sulle associazioni di tipo potrebbe-non potrebbe.
- Nei risultati del rapporto per l'oggetto B appaiono dei campi vuoti se l'oggetto A non ha l'oggetto B. Ad esempio, se un utente esegue un rapporto sugli account con o senza referenti, i campi dei referenti vengono visualizzati vuoti per gli account privi di referenti.
- Sui rapporti in cui l'oggetto A potrebbe o non potrebbe avere l'oggetto B, non è possibile utilizzare la condizione OR per filtrare più oggetti. Ad esempio, se si immette il criterio di filtro *`Il nome account inizia per M OR il nome del referente inizia per M`*, viene visualizzato un messaggio di errore per informare che il criterio di filtro non è corretto.
- L'opzione `Limite di riga` sui rapporti tabulari mostra soltanto i campi dell'oggetto principale sui rapporti creati a partire dai tipi di rapporto personalizzato, in cui l'oggetto A potrebbe e non potrebbe avere l'oggetto B. Ad esempio, in un account con o senza un rapporto referenti, vengono visualizzati solo i campi dell'account. I campi degli oggetti dopo un'associazione i tipo potrebbe-non potrebbe sui tipi di rapporto personalizzato non vengono visualizzati. Ad esempio, in un account con referenti con o senza rapporto sui casi, è possibile utilizzare soltanto i campi di account e referenti. Inoltre, i rapporti

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare o aggiornare tipi di rapporto personalizzato:
- "Gestisci tipi di rapporto personalizzato"

Per eliminare i tipi di rapporto personalizzato:
- "Modifica tutti i dati"

esistenti potrebbero non essere eseguiti o ignorare le impostazioni del `Limite di riga` se sono stati creati da tipi di rapporti personalizzati in cui le associazioni tra gli oggetti sono state modificate da oggetto A con oggetto B in oggetto A con o senza oggetto B.

## Definizione del layout dei campi per i rapporti creati a partire da un tipo di rapporto personalizzato

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare o aggiornare tipi di rapporto personalizzato:
- "Gestisci tipi di rapporto personalizzato"

Per eliminare i tipi di rapporto personalizzato:
- "Modifica tutti i dati"

Dopo avere definito un tipo di rapporto personalizzato e scelto le relative relazioni tra oggetti è possibile specificare i campi standard e personalizzati che possono essere visualizzati in un rapporto se questo viene creato o eseguito a partire da un tipo di rapporto personalizzato.

Nota: I campi personalizzati compaiono nei tipi di rapporto personalizzato solo se sono stati aggiunti al layout di pagina di quel tipo di rapporto.

1. Da Imposta, immettere *`Tipi di rapporto`* nella casella `Ricerca veloce`, quindi selezionare **Tipi di rapporto** per visualizzare la pagina Tutti i tipi di rapporto personalizzato.
2. Selezionare il tipo di rapporto personalizzato da modificare e fare clic su **Modifica layout** nella sezione Campi disponibili per i rapporti.

   È possibile fare clic su **Anteprima layout** per visualizzare in anteprima i campi che saranno riportati nella pagina Seleziona colonne di un rapporto personalizzato o eseguito a partire da questo tipo di rapporto.

   Nota: Quando si visualizza il layout in anteprima vengono visualizzati tutti i campi e gli oggetti, compresi quelli a cui l'utente non è autorizzato ad accedere. Non è invece possibile accedere ai dati memorizzati nei campi o negli oggetti a cui non si è autorizzati ad accedere.

3. Selezionare i campi dal riquadro di destra e trascinarli in una sezione di sinistra.

   Suggerimento: È possibile visualizzare i campi di un oggetto specifico selezionando un oggetto dall'elenco a discesa `Visualizza`.

4. Se lo si desidera, fare clic su **Aggiungi campi correlati tramite ricerca** per visualizzare la sovrapposizione Aggiungi campi tramite ricerca.

   Da qui è possibile aggiungere campi tramite la relazione di ricerca esistente fra l'oggetto selezionato nell'elenco a discesa `Visualizza` e gli altri oggetti.

   - Un campo di ricerca è un campo di un oggetto che visualizza informazioni di un altro oggetto, come ad esempio il campo `Nome referente` di un account.
   - Un tipo di rapporto personalizzato può contenere campi disponibili tramite la ricerca attraverso quattro livelli di relazioni di ricerca. Ad esempio, per un account, è possibile ottenere il titolare, il manager del titolare, il ruolo del manager e il ruolo controllante di tale ruolo.
   - Si possono aggiungere tramite ricerca solo i campi che sono associati agli oggetti inclusi nel tipo di rapporto personalizzato. Ad esempio, se si aggiunge l'oggetto account al tipo di rapporto personalizzato, sarà possibile aggiungere i campi di oggetti con cui gli account hanno una relazione di ricerca.
   - La selezione di un campo di ricerca nella sovrapposizione Aggiungi campi tramite ricerca potrebbe consentire di accedere a ulteriori campi di ricerca di altri oggetti con cui esiste una relazione di ricerca. Ad esempio, se si seleziona il campo `Nome referente` dai casi, successivamente sarà possibile selezionare il campo `Account` dai referenti poiché gli account hanno una relazione di ricerca con i referenti, che a loro volta presentano una relazione di ricerca con i casi.
   - I campi visualizzati nella sovrapposizione Aggiungi campi tramite ricerca non includono i campi di ricerca agli oggetti principali. Ad esempio, se gli account costituiscono l'oggetto principale del tipo di rapporto personalizzato, mentre i referenti costituiscono

l'oggetto secondario, la sovrapposizione Aggiungi campi tramite ricerca non consente di visualizzare i campi di ricerca dai referenti agli account.

- I campi aggiunti al layout tramite il link **Aggiungi campi correlati tramite ricerca** vengono inclusi automaticamente nella sezione dell'oggetto da cui rappresentano un campo di ricerca. Ad esempio, se si aggiunge il campo `Referente` come campo di ricerca a partire dagli account, il campo `Referente` verrà automaticamente incluso nella sezione Account. L'opzione di trascinamento di un campo in una sezione qualsiasi rimane comunque disponibile.
- I campi aggiunti automaticamente tramite ricerca vengono visualizzati con l'icona di ricerca nel layout del campo del tipo di rapporto personalizzato.
- Ridurre il tempo impiegato dall'utente per cercare i campi con cui generare un rapporto raggruppando insieme campi simili nei layout dei campi dei tipi di rapporto personalizzato. È possibile creare nuove sezioni di pagina in cui raggruppare i campi correlati fra di loro, nonché raggruppare i campi in base a pagine dei dettagli e tipi di record specifici.
- Se si includono attività come oggetto principale di un tipo di rapporto personalizzato, è possibile aggiungere solo campi di ricerca da attività ad account nel layout Seleziona colonne del tipo di rapporto personalizzato.

5. Disporre i campi all'interno delle sezioni così come dovrebbero comparire agli utenti.

   I campi che non vengono trascinati in una sezione non saranno disponibili quando si generano rapporti a partire da questo tipo di rapporto.

6. Fare clic su **Anteprima layout** e utilizzare la legenda per determinare i campi inclusi nel layout, aggiunti al rapporto per impostazione predefinita e aggiunti al layout tramite una relazione di ricerca.

   Avvertenza: gli utenti possono visualizzare i campi di riepilogo di roll-up nei rapporti che includono dati di campi che non sono autorizzati a visualizzare. Ad esempio, un utente non autorizzato a visualizzare il campo `Prezzo` di un prodotto opportunità può visualizzare il campo `Prezzo totale` dei rapporti opportunità se è autorizzato ad accedere al campo `Prezzo totale`.

7. Per rinominare o impostare i campi selezionati per impostazione predefinita per gli utenti, selezionare uno o più campi, quindi fare clic su **Modifica proprietà**.

   - Fare clic sulla casella di controllo `Selezionato per impostazione predefinita` accanto a uno o più campi.

     I campi selezionati per impostazione predefinita vengono visualizzati automaticamente con l'icona della casella di controllo (✓) nel layout del campo del tipo di rapporto personalizzato.

   - Modificare il testo nel campo `Visualizza come` accanto al campo da rinominare.

     Nota: I campi rinominati degli oggetti standard, come pure gli oggetti standard rinominati, non compaiono con i nuovi nomi nel layout dei campi del tipo di rapporto personalizzato. I campi rinominati degli oggetti standard e gli oggetti standard rinominati compaiono con il nuovo nome sul rapporto e nella pagina di anteprima, disponibile facendo clic su **Anteprima layout**.

8. Per rinominare le sezioni, fare clic su **Modifica** accanto a una sezione esistente o creare una nuova sezione facendo clic su **Crea nuova sezione**.
9. Fare clic su **Salva**.

## Gestione dei tipi di rapporto personalizzato

Una volta creato un tipo di rapporto personalizzato è possibile personalizzarlo, modificarlo ed eliminarlo.

Da Imposta, immettere *`Tipi di rapporto`* nella casella `Ricerca veloce`, quindi selezionare **Tipi di rapporto** per visualizzare la pagina Tutti i tipi di rapporto personalizzato, che mostra l'elenco dei tipi di rapporto personalizzato definiti per l'organizzazione.

- Selezionare una visualizzazione elenco dall'elenco a discesa `Visualizza` per passare direttamente alla pagina di elenco specificata oppure fare clic su **Crea nuova visualizzazione** per definire una visualizzazione personalizzata.
- Definire un nuovo tipo di rapporto personalizzato facendo clic su **Nuovo tipo di rapporto personalizzato**.
- Aggiornare il nome, la descrizione, la categoria e lo stato di utilizzo di un tipo di rapporto personalizzato facendo clic su **Modifica** accanto al nome del tipo di rapporto personalizzato.
- Eliminare un tipo di rapporto personalizzato facendo clic su **Canc** accanto al nome del tipo di rapporto personalizzato. Tutti i dati memorizzati nel tipo di rapporto personalizzato saranno eliminati e non potranno essere ripristinati dal Cestino.

  Importante: quando si elimina un tipo di rapporto personalizzato vengono eliminati anche tutti i rapporti basati su quel tipo. Tutti gli eventuali componenti di cruscotti digitali creati a partire da un rapporto basato su un tipo di rapporto personalizzato che è stato eliminato mostreranno un messaggio di errore quando vengono visualizzati.

- Visualizzare informazioni dettagliate su un tipo di rapporto personalizzato e personalizzarlo ulteriormente facendo clic sul nome del tipo di rapporto personalizzato.

  Dopo avere fatto clic sul nome del tipo di rapporto personalizzato è possibile:

  - Aggiornare le relazioni tra oggetti che un rapporto può visualizzare quando viene eseguito a partire da quel tipo di rapporto personalizzato.
  - Modificare il layout di pagina del tipo di rapporto personalizzato per specificare quali campi standard e personalizzati possono essere visualizzati nel rapporto se questo viene creato o eseguito a partire da quel tipo di rapporto personalizzato.
  - Visualizzare in anteprima come appariranno i campi agli utenti nei rapporti eseguiti a partire dal tipo di rapporto personalizzato facendo clic su **Anteprima layout** nella sezione Campi esposti per i rapporti.
  - Creare un nuovo tipo di rapporto personalizzato con gli stessi campi e le relazioni tra oggetti del tipo di rapporto personalizzato selezionato facendo clic su **Clona**.
  - Rinominare i campi nel rapporto.
  - Impostare i campi selezionati per impostazione predefinita.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare o aggiornare tipi di rapporto personalizzato:
- "Gestisci tipi di rapporto personalizzato"

Per eliminare i tipi di rapporto personalizzato:
- "Modifica tutti i dati"

Durante la modifica di un rapporto, il tipo di rapporto è visualizzato sopra il nome del rapporto nel Generatore di rapporti. Il tipo di rapporto non è visualizzato nella pagina di esecuzione del rapporto.

1. Tipo di rapporto
2. Nome rapporto

Nota: Se è attivata l'Area di lavoro traduzione per l'organizzazione, è possibile tradurre i tipi di rapporto personalizzato per gli utenti internazionali.

## Limiti dei tipi di rapporto

I tipi di rapporto personalizzato sono soggetti ad alcuni limiti per garantirne le prestazioni e la fruibilità.

- A un tipo di rapporto personalizzato è possibile aggiungere fino a 1000 campi. Un contatore in cima alla fase Layout di pagina mostra il numero corrente di campi inclusi. Se sono presenti troppi campi, non è possibile salvare il layout.
- Ai tipi di rapporto personalizzato non è possibile aggiungere i seguenti campi:
  - Campi Pianificazione prodotto
  - Campi cronologia
  - Campi account personali
  - Il campo `Durata` di casi e opportunità
- Un tipo di rapporto personalizzato può contenere fino a 60 riferimenti a oggetti. Ad esempio, se il limite massimo selezionato di relazioni tra oggetti per un tipo di rapporto è quattro, è possibile selezionare campi tramite ricerca da altri 56 oggetti. Tuttavia, gli utenti riceveranno un messaggio di errore se eseguono un rapporto da un tipo di rapporto personalizzato e il rapporto contiene colonne da oltre 20 oggetti diversi.
- I riferimenti agli oggetti si possono utilizzare come i quattro oggetti principali, come origini dei campi tramite la ricerca o come oggetti utilizzati per attraversare le relazioni. Ogni oggetto a cui si fa riferimento viene conteggiato nel limite massimo anche se da esso non viene scelto alcun campo. Ad esempio, se si esegue una ricerca dall'account al titolare dell'account e al ruolo del titolare dell'account, ma non si seleziona alcun campo del titolare, tutti gli oggetti a cui si fa riferimento vengono contati ai fini del limite di 60.
- Nei rapporti eseguiti da tipi di rapporto personalizzato che includono casi non viene visualizzato l'elenco a discesa `Unità`, che consente agli utenti di visualizzare i valori temporali di determinati campi dei casi in base alle ore, ai minuti o ai giorni.
- I tipi di rapporto associati agli oggetti personalizzati nell'elenco Oggetti personalizzati eliminati vengono calcolati ai fini del conteggio del numero massimo di tipi di rapporto che possono essere creati.

# Abilitazione della condivisione ottimizzata per i rapporti e i cruscotti digitali

Quando si abilita la condivisione delle applicazioni analitiche, Salesforce converte i livelli esistenti di accesso alle cartelle degli utenti a nuovi e più dettagliati livelli di accesso.

Nota: se l'organizzazione è stata creata dopo il rilascio Summer '13 di Salesforce, si dispone già della condivisione delle cartelle analitiche. Se l'organizzazione esisteva prima del rilascio Summer '13, seguire questa procedura per mettere a disposizione degli utenti la condivisione delle cartelle.

Quando è in vigore la condivisione delle analitiche, per impostazione predefinita tutti gli utenti all'interno dell'organizzazione dispongono dell'accesso come Visualizzatori ai rapporti e ai cruscotti digitali che vengono condivisi con loro. Gli utenti possono disporre di un accesso più ampio se sono Responsabili o Editor di una data cartella, oppure se dispongono di ulteriori autorizzazioni utente amministrative. L'accesso di ogni utente alle cartelle con la nuova funzionalità è basato sulla combinazione delle autorizzazioni utente e di accesso alla cartella di cui disponeva prima dell'abilitazione della condivisione ottimizzata delle cartelle.

1. Da Imposta, immettere *Condivisione cartella* nella casella Ricerca veloce, quindi selezionare **Condivisione cartella**.
2. Selezionare **Abilita i livelli di accesso per la condivisione delle cartelle di rapporti e cruscotti digitali**.
3. Fare clic su **Condivisione cartella rapporti e cruscotti digitali**.

Importante: Se si ritorna al vecchio modello di condivisione delle cartelle, le cartelle dei rapporti e dei cruscotti digitali già esistenti ritornano allo stato precedente.

- Se una cartella esisteva prima dell'abilitazione della condivisione delle cartelle analitiche, le sue proprietà e le sue impostazioni di condivisione vengono riportate allo stato precedente.
- Se una cartella è stata creata mentre era in vigore la condivisione ottimizzata delle cartelle analitiche, non è visibile nell'elenco delle cartelle e le sue impostazioni di condivisione vengono rimosse. Le autorizzazioni utente amministrative rimangono in vigore.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **tutte** le versioni tranne **Database.com** Edition

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni di condivisione delle cartelle analitiche:

- "Visualizza impostazione e configurazione"

Per modificare le impostazioni di condivisione delle cartelle analitiche:

- "Personalizza applicazione"

## Configurazione dei rapporti con trend storico

Per mettere a disposizione degli utenti i rapporti con trend storico, configurare mediante dei filtri la quantità di dati che viene acquisita per i rapporti con trend storico. Quindi selezionare i campi necessari per i rapporti storici.

Definire le dimensioni dei dati di trend storico in modo che risultino sufficientemente utili per gli utenti, senza però superare i limiti di spazio disponibili. Esaminare i campi contenenti dati cronologici utili e i campi contenenti dati che è possibile ignorare.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

AUTORIZZAZIONI UTENTE

Per creare, modificare ed eliminare i rapporti:

- "Crea e personalizza rapporti"

  E

  "Generatore di rapporti"

Importante: Se si conservano i dati cronologici, la quantità complessiva di dati da memorizzare aumenta. L'effetto dipende dalle modalità operative della propria organizzazione. Si supponga che un utente aggiorni lo stato di un tipico record opportunità ogni uno o due giorni. I dati di trend storico del campo Stato nell'oggetto Opportunità occuperanno più spazio di quanto ne occuperebbero se il record venisse modificato una o due volte al mese. Se uno degli oggetti di cui si rileva il trend storico rischia di superare il limite dei dati, si riceverà un avviso email.

1. Da Imposta, immettere *Trend storico* nella casella `Ricerca veloce`, quindi selezionare **Trend storico**.
2. Selezionare l'oggetto su cui si desiderano eseguire rapporti con trend storico.

   È possibile selezionare Opportunità, Casi, Voce previsioni e un massimo di tre oggetti personalizzati.

   Nota: i rapporti con trend storico sono disponibili solo con le previsioni collaborative, non con le previsioni personalizzabili.

3. Selezionare **Abilita trend storico**.
4. Utilizzare i filtri in **Configura dati** per specificare la quantità totale di dati che è possibile utilizzare per creare rapporti con trend storico.

   Nota: È possibile ridurre i dati storici per Opportunità, Casi e oggetti personalizzati. Per Voci previsioni, i dati disponibili vengono selezionati per conto dell'utente.

   Ad esempio, per ridurre i dati archiviati per i rapporti Opportunità, escludere le trattative con meno probabilità di successo, impostando `Fase non uguale a` *Potenziale*.

5. In **Seleziona campi**, scegliere fino a otto campi da rendere disponibili per i rapporti con trend storico.

   È possibile selezionare questi campi durante la creazione di rapporti con trend storico.

   Nota:

   - per i rapporti Opportunità sono preselezionati cinque campi: Ammontare, Data chiusura, Categoria di previsione, Probabilità e Fase. È possibile aggiungerne altri tre.
   - Per le previsioni, tutti gli otto campi disponibili sono preselezionati.

Dopo aver abilitato il trend storico, sarà disponibile un nuovo tipo di rapporto personalizzato per la creazione dei rapporti. Se si abilita il trend storico su un nuovo campo, il campo viene aggiunto automaticamente al layout dei rapporti con trend storico.

Quando si disattiva il trend storico, tenere presente quanto segue.

- La disattivazione del trend storico per un campo nasconde i dati cronologici del campo. Se si riattiva il trend storico, sarà possibile visualizzare nuovamente i dati cronologici del campo, inclusi i dati creati dopo la disattivazione del trend storico.
- La disattivazione del trend storico per un oggetto elimina tutti i dati cronologici e le impostazioni di configurazione dell'oggetto. Viene eliminato anche il tipo di rapporto con trend storico dell'oggetto e tutti i rapporti creati utilizzando quel tipo di rapporto.

- Se si disattiva il trend storico per un campo e si elimina il campo, i dati cronologici del campo non saranno più disponibili anche se si riattiva il trend storico.

Nota:

- I campi storici disponibili per i singoli utenti dipendono dai campi a cui gli utenti sono autorizzati ad accedere. Se le autorizzazioni cambiano e non si riesce più a visualizzare un determinato campo, anche i dati cronologici di quel campo diventano invisibili.
- Ogni campo storico ha la stessa protezione a livello di campo del suo campo controllante. Se le autorizzazioni a livello di campo del campo controllante cambiano, le autorizzazioni del campo storico cambiano di conseguenza.

# Aggiornamento della creazione guidata rapporto

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni di rapporti e cruscotti digitali:
- "Personalizza applicazione"

Il Generatore di rapporti, un efficace editor con trascinamento della selezione, è lo strumento standard per la creazione e la modifica dei rapporti. Se la propria organizzazione sta ancora utilizzando la vecchia Creazione guidata rapporto, è opportuno eseguire l'aggiornamento al Generatore di rapporti.

- Tutti i profili hanno accesso al Generatore di rapporti per impostazione predefinita. È possibile che l'autorizzazione "Generatore di rapporti" negli insiemi di autorizzazioni e nei profili e gli oggetti Insieme di autorizzazioni e Profilo rimangano visibili nell'API anche se l'aggiornamento sovrascrive tali impostazioni.
- La precedente procedura guidata per la creazione dei rapporti è disponibile soltanto per gli utenti in modalità di accessibilità.
- Il Generatore di rapporti è disponibile per le organizzazioni che utilizzano le versioni Group Edition e Professional Edition.
- Sono disponibili i grafici a dispersione, un nuovo tipo di grafico per i rapporti.

Le nuove organizzazioni ricevono automaticamente l'ultima versione del Generatore di rapporti. Se la sezione Aggiornamento del Generatore di rapporti non è visibile nella pagina Impostazioni dell'interfaccia utente, significa che l'aggiornamento è già stato abilitato per l'organizzazione.

Assegnare l'autorizzazione "Generatore di rapporti" a tutti gli utenti tramite profili o insiemi di autorizzazioni non equivale ad abilitare il Generatore di rapporti per tutta l'organizzazione. Per abilitare il Generatore di rapporti per la propria organizzazione, attenersi alla seguente procedura.

Importante: L'aggiornamento **non ha effetto** sui rapporti esistenti. Tuttavia, dopo aver eseguito l'aggiornamento, non è possibile tornare alla precedente procedura guidata relativa ai rapporti.

1. Da Imposta, immettere *Rapporti* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni rapporti e cruscotti digitali**.
2. Rivedere la sezione Aggiornamento del Generatore di rapporti della pagina e fare clic su **Abilita**. Se il pulsante non compare, il Generatore di rapporti è già stato abilitato per tutta l'organizzazione.
3. Confermare la scelta facendo clic su **Sì, abilita il Generatore di rapporti per tutti gli utenti**.

# Gestione della fatturazione e delle licenze

Checkout contiene informazioni sull'account Salesforce della propria organizzazione, incluse le licenze, i dati di fatturazione, gli ordini, le fatture e gli estratti conto.

Per accedere a Checkout, da Imposta, immettere *Checkout* nella casella `Ricerca veloce`, selezionare **Checkout** e scegliere **Continua in Checkout**.

Nota: gli utenti che dispongono dell'autorizzazione "Gestisci fatturazione" hanno automaticamente accesso a Checkout. Questi utenti possono anche concedere l'accesso ad altri utenti all'interno dell'organizzazione; vedere Concessione dell'accesso a Checkout a pagina 127.

Da Checkout, è possibile:

- Ordinare altre licenze e altri prodotti.
- Modificare i dati di fatturazione di un contratto attivo.
- Modificare i dati della carta di credito associata a un contratto attivo.
- Visualizzare gli ordini e le fatture della propria organizzazione.
- Visualizzare i preventivi salvati in precedenza, sia i preventivi creati da Salesforce, sia quelli creati da un agente di vendita.
- Inviare ordini per acquistare nuovi prodotti.
- Contattare Salesforce per richiedere assistenza alla vendita.
- Registrare un caso per eventuali domande, problemi o questioni relative a Checkout.

Per istruzioni dettagliate sull'uso di Checkout, vedere la Guida dell'utente di Checkout.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

## Acquisto di più licenze per gli utenti

Gli utenti con Checkout abilitato possono aggiungere licenze per l'organizzazione in qualsiasi momento mentre un contratto è in vigore. Se la propria organizzazione non dispone di un accesso self-service a Checkout, inviare una richiesta al rappresentante Salesforce.

Nota: in qualsiasi fase del processo di creazione del preventivo è possibile fare clic su **Richiesta di assistenza commerciale** per contattare un addetto alle vendite Salesforce.

1. Da Imposta, immettere *Checkout* nella casella `Ricerca veloce`, quindi selezionare **Checkout** e fare clic su **Continua in Checkout**.
2. Fare clic su **Aggiungi altri prodotti**.
3. Per visualizzare tutti i prodotti supportati dall'organizzazione, fare clic su **Tutti i prodotti disponibili**.
4. Immettere il numero di abbonamenti alle licenze che si desidera acquistare.

   Se le licenze vengono acquistate a metà di un ciclo di fatturazione, l'abbonamento viene ripartito proporzionalmente in base al numero di giorni rimasti in tale ciclo di fatturazione. Il `Prezzo totale` riflette il `Prezzo unitario mensile` per il periodo di validità dell'ordine, specificato per i prodotti. Ad esempio, se gli abbonamenti di un ordine iniziano il 14/5/2013 e terminano il 7/5/2014, il `Prezzo totale` rifletterà il `Prezzo unitario mensile` per 11,8 mesi.
5. Fare clic su **Procedi con l'emissione dell'ordine**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Personal Edition**, **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Unlimited Edition**, **Performance Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per acquistare ulteriori licenze utente:

- "Gestisci fatturazione"

6. Controllare l'ordine e i dati del pagamento. Fare clic sulla matita se è necessario apportare modifiche.
7. Leggere e confermare che si accetta l'Accordo Quadro di Sottoscrizione ed eventuali altri termini e contratti richiesti.

   In base al contratto con Salesforce e ai prodotti acquistati, potrebbe essere necessario accettare termini specifici del contratto o dei prodotti.
8. Fare clic su **Emetti ordine**.

VEDERE ANCHE:

Gestione della fatturazione e delle licenze
Concessione dell'accesso a Checkout
Eliminazione di licenze utente
Modifica dei dati di fatturazione dell'organizzazione
Guida dell'utente di Checkout
Conversione di una versione di prova mediante Checkout

## Eliminazione di licenze utente

Salesforce non supporta l'uso di Checkout per ridurre il numero di licenze di un'organizzazione.

Per eliminare delle licenze, rivolgersi al rappresentante Salesforce.

Nota: la disattivazione di account utente non modifica il numero di licenze utente addebitate alla propria società.

VEDERE ANCHE:

Gestione della fatturazione e delle licenze
Concessione dell'accesso a Checkout
Acquisto di più licenze per gli utenti

## Modifica dei dati di fatturazione dell'organizzazione

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

Per modificare i dati di fatturazione e pagamento della propria organizzazione, è necessario disporre dell'accesso a Checkout. Se la propria organizzazione non dispone di un accesso self-service a Checkout, inviare una richiesta al rappresentante Salesforce.

1. Da Imposta, immettere *`Checkout`* nella casella `Ricerca veloce`, quindi selezionare **Checkout**.
2. Fare clic su **Continua in Checkout**.
3. Fare clic su **Cambia indirizzo di fatturazione contratto**.
4. Aggiornare l'indirizzo e i dati di contatto dell'organizzazione secondo necessità.
5. Fare clic su **Salva**.

Per istruzioni dettagliate sull'uso di Checkout, vedere la Guida dell'utente di Checkout.

VEDERE ANCHE:

Gestione della fatturazione e delle licenze

## Modifica dei dati della carta di credito o di addebito diretto

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

Per modificare i dati della carta di credito o di addebito diretto, è necessario avere accesso a Checkout. Se la propria organizzazione non dispone di un accesso self-service a Checkout, inviare una richiesta al rappresentante Salesforce.

Per accedere a Checkout, da Imposta, immettere *Checkout* nella casella `Ricerca veloce`, selezionare **Checkout** e quindi fare clic su **Continua in Checkout**.

Per istruzioni dettagliate sulla modifica dei dati di pagamento in Checkout, vedere la Guida dell'utente di Checkout.

Nota: La fattura non può essere pagata online. Se il proprio account presenta un saldo scoperto, l'ammontare verrà addebitato sulla carta di credito o di addebito diretto nel giro di 24 ore. Per pagare una fattura tramite carta di credito, contattare il reparto di assistenza clienti di Salesforce.

VEDERE ANCHE:

Gestione della fatturazione e delle licenze

## Visualizzazione di note di accredito, rendiconti e fatture

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

Per visualizzare le note di accredito, i rendiconti e le fatture della propria organizzazione occorre essere autorizzati ad accedere a Checkout. Se la propria organizzazione non dispone di un accesso self-service a Checkout, inviare una richiesta al rappresentante Salesforce.

Nella pagina dei dettagli di una nota di accredito, di un rendiconto o di una fattura è possibile stampare, registrare casi per indagare sugli eventuali problemi o contattare Salesforce.

Per accedere a Checkout, da Imposta immettere *Checkout* nella casella `Ricerca veloce`, selezionare **Checkout** e quindi fare clic su **Continua in Checkout**.

Nota: È possibile che l'account non includa un saldo iniziale a seconda della durata selezionata. È possibile aprire tutti i pagamenti, le fatture e le note di accredito per visualizzare ulteriori dettagli o stamparli.

Per istruzioni dettagliate sull'uso di Checkout, vedere la Guida dell'utente di Checkout.

VEDERE ANCHE:

Gestione della fatturazione e delle licenze

# Concessione dell'accesso a Checkout

Gli utenti che dispongono dell'autorizzazione "Gestisci fatturazione" hanno accesso a Checkout quando questo è abilitato per l'organizzazione. Questi utenti possono anche concedere l'accesso ad altri utenti all'interno dell'organizzazione. Gli utenti con accesso Checkout possono acquistare licenze Salesforce, licenze per applicazioni AppExchange e altri prodotti correlati. Inoltre, all'interno di Checkout gli utenti possono visualizzare i preventivi, i prodotti installati, gli ordini, le fatture, i pagamenti e i contratti dell'organizzazione.

Per concedere a un utente l'accesso a Checkout:

1. Da Imposta, immettere *`Utenti`* nella casella `Ricerca veloce`, quindi selezionare **Utenti**.
2. Fare clic sul nome utente desiderato per aprire la pagina dei dettagli di quell'utente.
3. Fare clic su **Modifica**.
4. Selezionare la casella di controllo `Checkout abilitato`. L'utente viene informato tramite email dell'attivazione del proprio account Checkout e della possibilità di accedervi.

VEDERE ANCHE:

Gestione della fatturazione e delle licenze
Acquisto di più licenze per gli utenti
Guida dell'utente di Checkout

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per concedere l'accesso a Checkout:

- "Gestisci fatturazione"

Per modificare gli utenti:

- "Gestisci utenti interni"

# Panoramica sugli aggiornamenti critici

Salesforce pubblica aggiornamenti periodici che consentono di migliorare le prestazioni, la logica e la fruibilità di Salesforce, ma che potrebbero avere un impatto sulle personalizzazioni esistenti. Quando questi aggiornamenti diventano disponibili, Salesforce li elenca in Imposta **Aggiornamenti critici** e visualizza un messaggio quando gli amministratori vanno alla sezione Imposta.

Per garantire una transizione senza problemi, ogni aggiornamento prevede un periodo di adesione durante il quale è possibile attivare e disattivare l'aggiornamento per un numero illimitato di volte in modo da poter valutare il suo impatto sull'organizzazione e modificare secondo necessità le personalizzazioni su cui l'aggiornamento ha effetto. Tale periodo termina alla data di attivazione automatica, quando Salesforce attiva l'aggiornamento in modo definitivo.

Avvertenza: Salesforce consiglia di testare l'aggiornamento attivandolo nell'organizzazione Sandbox per sviluppatori o nell'ambiente di produzione durante gli orari di attività ridotta.

Per gestire gli aggiornamenti critici, da Imposta, fare clic su **Aggiornamenti critici**. Da questa pagina è possibile visualizzare il riepilogo, lo stato e la data di attivazione automatica per tutti gli aggiornamenti che Salesforce non ha attivato in modo definitivo. Per visualizzare più dettagli sull'aggiornamento, compreso un elenco delle personalizzazioni dell'organizzazione che potrebbero essere influenzate dall'aggiornamento, fare clic su **Esamina**.

Se un aggiornamento contiene un link **Attiva**, fare clic sul link per testare l'aggiornamento nel proprio ambiente Sandbox o di produzione prima che Salesforce lo attivi automaticamente.

EDIZIONI

Disponibile nelle versioni: Lightning Experience e Salesforce Classic

Disponibile in: tutte le versioni

AUTORIZZAZIONI UTENTE

Per visualizzare gli aggiornamenti critici:
- "Visualizza impostazione e configurazione"

Per attivare gli aggiornamenti critici:
- "Modifica tutti i dati"

  E

  "Personalizza applicazione"

## Note sugli aggiornamenti critici

- Salesforce analizza l'organizzazione per determinare se un aggiornamento critico può influenzare le personalizzazioni. Se le personalizzazioni non sono interessate, Salesforce attiva automaticamente l'aggiornamento nell'organizzazione.
- Alla data prevista per l'attivazione automatica, Salesforce attiva l'aggiornamento in modo permanente. Dopo l'attivazione automatica, l'aggiornamento non può più essere disattivato.
- La pagina dei dettagli di ciascun aggiornamento descrive in che modo le personalizzazioni potrebbero essere influenzate e come è possibile correggere gli eventuali funzionamenti indesiderati.
- La prima volta che si accede al menu di impostazione dopo che è diventato disponibile un aggiornamento critico, Salesforce visualizza un messaggio. Tale messaggio consente di scegliere se Salesforce deve visualizzare gli aggiornamenti immediatamente o visualizzare un promemoria in un secondo tempo.

# Panoramica sulle divisioni

Le divisioni consentono di segmentare i dati dell'organizzazione in sezioni logiche, rendendo ricerche, rapporti e visualizzazioni elenco più significative per gli utenti. Ad esempio, è possibile creare un rapporto che mostri esclusivamente le opportunità per la divisione nordamericana, per ottenere dati di vendita accurati solo per il team delle vendite nordamericano. Le divisioni sono utili in quelle organizzazioni che dispongono di ingenti quantità di dati.

Nota: Le divisioni non limitano l'accesso ai dati e non svolgono una funzione di protezione.

Le divisioni possono essere assegnate agli utenti e ad altri record.

- **Divisione a livello di record** - Divisione è un campo disponibile nei singoli record che contrassegna il record come appartenente a una determinata divisione. Un record può

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

appartenere alla divisione creata dall'amministratore oppure alla divisione "globale" standard che viene creata automaticamente quando si abilitano le divisioni. Un record può appartenere a una sola divisione alla volta.

- **Divisione predefinita**- Agli utenti viene assegnata una divisione predefinita che viene applicata ai nuovi account, lead, oggetti personalizzati creati dagli utenti e abilitati per le divisioni.
- **Divisione di lavoro** - Se si dispone dell'autorizzazione "Limita per divisione", si imposta la divisione utilizzando l'elenco a discesa nell'intestazione laterale. In tal modo, nelle ricerche vengono restituiti solo i dati della divisione di lavoro corrente. È possibile cambiare la divisione di lavoro in qualsiasi momento. Se non si dispone dell'autorizzazione "Limita per divisione", i record verranno sempre visualizzati in tutte le divisioni.

L'effetto dell'uso delle divisioni è riepilogato nella seguente tabella.

| Area | Descrizione |
| --- | --- |
| Ricerca | Se si dispone dell'autorizzazione "Limita per divisione":<br>• Nella ricerca dall'intestazione laterale è possibile selezionare una singola divisione oppure tutte le divisioni.<br>• Nella ricerca avanzata è possibile selezionare una singola divisione oppure tutte le divisioni.<br>• Nella ricerca globale è possibile eseguire la ricerca in una singola divisione oppure in tutte le divisioni.<br>• Per le ricerche nelle finestre di dialogo di ricerca, i risultati possono includere i record della divisione selezionata nell'elenco a discesa della finestra di dialogo di ricerca.<br>Nota: Tutte le ricerche all'interno di una specifica divisione di lavoro comprendono anche la divisione globale. Ad esempio, se si cerca all'interno di una divisione chiamata Divisione occidentale, i risultati comprenderanno i record trovati sia nella Divisione occidentale che nella divisione globale.<br>Se non si dispone dell'autorizzazione "Limita per divisione", i risultati di ricerca includono sempre i record di tutte le divisioni. |
| Visualizzazioni elenco | Se si dispone dell'autorizzazione "Limita per divisione", le visualizzazioni elenco includono solo i record della divisione specificata al momento della creazione o della modifica della visualizzazione elenco. Le visualizzazioni elenco che non includono tutti i record, ad esempio Casi aperti personali, includono i record di tutte le divisioni.<br>Se non si dispone dell'autorizzazione "Limita per divisione", le visualizzazioni elenco includono sempre i record di tutte le divisioni. |
| Chatter | Chatter non supporta le divisioni. Ad esempio, non è possibile utilizzare feed Chatter separati per divisioni diverse. |
| Rapporti | Se si dispone dell'autorizzazione "Limita per divisione", è possibile impostare le opzioni dei rapporti in modo da includervi i record di una sola divisione o di tutte le divisioni. I rapporti che utilizzano filtri standard, ad esempio Casi personali o Account del team |

| Area | Descrizione |
| --- | --- |
| | personale, mostrano i record di tutte le divisioni e non è possibile limitarli ulteriormente a una divisione specifica.<br><br>Se non si dispone dell'autorizzazione "Limita per divisione", i rapporti includono sempre i record di tutte le divisioni. |
| Visualizzazione di record ed elenchi correlati | Quando si visualizza la pagina dei dettagli di un record, negli elenchi correlati vengono visualizzati tutti i record associati a cui si ha accesso, indipendentemente dalla divisione. |
| Creazione di nuovi record | Quando si creano nuovi account, lead o oggetti personalizzati abilitati per le divisioni, la divisione viene impostata automaticamente sulla divisione predefinita, a meno che non si ignori questa impostazione.<br><br>Quando si creano nuovi record correlati a un account o a un altro record che dispone già di una divisione, il nuovo record viene assegnato alla divisione del record esistente. Ad esempio, se si crea un record oggetto personalizzato che è il record "dettaglio" in una relazione record principale-record dettaglio con un oggetto personalizzato per cui sono abilitate le divisioni, il record viene assegnato alla divisione del record principale.<br><br>Quando si creano record che non sono correlati ad altri record, ad esempio opportunità private o referenti non correlati a un account, la divisione viene impostata automaticamente su quella globale. |
| Modifica di record | Quando si modificano account, lead o oggetti personalizzati che sono abilitati per le divisioni, è possibile modificare la divisione. Anche tutti i record che sono associati tramite una relazione record principale-record dettaglio vengono automaticamente trasferiti alla nuova divisione. Ad esempio, i referenti e le opportunità vengono trasferiti alla nuova divisione dell'account associato e gli oggetti personalizzati del record dettaglio vengono trasferiti alla nuova divisione del rispettivo record principale.<br><br>Quando si modificano altri tipi di record, non è possibile modificare l'impostazione della divisione. |
| Oggetti personalizzati | Quando si abilitano le divisioni per un oggetto personalizzato, inizialmente Salesforce assegna alla divisione globale tutti i record per quell'oggetto personalizzato.<br><br>Quando si crea un record oggetto personalizzato:<br>• Se l'oggetto personalizzato è abilitato per le divisioni, il record adotta la divisione predefinita dell'utente.<br>• Se l'oggetto personalizzato è il record dettaglio in una relazione record principale-record dettaglio con un oggetto personalizzato abilitato per le divisioni, il record adotta la divisione del record principale. |

| Area | Descrizione |
| --- | --- |
| Relazioni | Se si converte una relazione di ricerca in una relazione record principale-record dettaglio, i record dettaglio perdono la divisione corrente ed ereditano quella del record principale. Se si converte una relazione record principale-record dettaglio in una relazione di ricerca, la divisione degli eventuali record dettaglio è determinata dal record principale precedente. Se si elimina una relazione record principale-record dettaglio, la divisione degli eventuali record dettaglio è determinata dal record principale precedente. |

VEDERE ANCHE:

Impostazione delle divisioni

Creazione e modifica di divisioni

Modifica della divisione predefinita degli utenti

Trasferimento di più record tra le divisioni

Generazione di rapporti con le divisioni

## Impostazione delle divisioni

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare o modificare divisioni:

- "Modifica tutti i dati"

Quando si impostano le divisioni, è necessario creare le divisioni e assegnare record alle stesse per accertarsi che i dati vengano classificati in modo efficace.

Prima di utilizzare la funzione delle divisioni per l'organizzazione, è necessario abilitarla. Se si utilizza un oggetto standard, contattare Salesforce per abilitare le divisioni per la propria organizzazione. Per gli oggetti personalizzati, selezionare `Abilita divisioni` nella pagina di definizione di un oggetto personalizzato per abilitare le divisioni.

1. Pianificare le divisioni necessarie in base al modo in cui si desidera segmentare i dati.
   Ad esempio, può essere necessario utilizzare una divisione per tutti i record appartenenti al team di vendita del Nord America e una divisione per il team di vendita europeo.

   100

2. Creare divisioni per l'organizzazione. Tutti i record esistenti vengono assegnati alla divisione "Globale" per impostazione predefinita. È possibile modificare il nome predefinito della divisione, creare divisioni aggiuntive e spostare record di utenti e dati tra le divisioni.
3. Trasferire lead, account e oggetti personalizzati nelle divisioni appropriate. Quando i record vengono assegnati a una divisione, i record associati vengono assegnati alla stessa divisione. Ad esempio, se si modifica la divisione assegnata a un account, i record correlati, quali referenti e opportunità, vengono assegnati alla stessa divisione.
4. Aggiungere campi divisione ai layout di pagina.
5. Aggiungere divisioni alla protezione a livello di campo.
6. Impostare la divisione predefinita per tutti gli utenti. I nuovi account e lead vengono assegnati alla divisione predefinita dell'utente a meno che l'utente non lo assegni esplicitamente a un'altra divisione. I nuovi record correlati ai record esistenti vengono assegnati alla divisione dei record esistenti.

7. Abilitare l'autorizzazione "Limita per divisione" per gli utenti che devono essere in grado di limitare le visualizzazioni elenco per divisione, eseguire ricerche all'interno di una divisione o creare rapporti in una divisione.

   Gli utenti senza autorizzazione "Limita per divisione" dispongono comunque di una divisione predefinita a livello di utente, possono visualizzare i campi divisione, modificare la divisione per un record e specificare una divisione durante la creazione dei record.

VEDERE ANCHE:

Panoramica sulle divisioni

Creazione e modifica di divisioni

Trasferimento di più record tra le divisioni

Modifica della divisione predefinita degli utenti

## Creazione e modifica di divisioni

La creazione di divisioni logiche per l'organizzazione consente di segmentare i record per facilitare ricerche e creazione di rapporti.

Le divisioni devono essere abilitate per l'organizzazione.

Tutti i record vengono inizialmente assegnati alla divisione predefinita "Globale" finché l'utente non definisce la divisione. È possibile creare un massimo di 100 divisioni, incluse quelle eventualmente inattive.

1. Da Imposta, immettere *Gestisci divisioni* nella casella `Ricerca veloce`, quindi selezionare **Gestisci divisioni**.
2. Fare clic su **Nuova** per creare una divisione oppure su **Modifica** per modificarne una esistente.
3. Immettere il nome della divisione.
4. Selezionare la casella di controllo per rendere attiva la divisione.

   Nota: Non è possibile rendere inattiva una divisione se a questa sono state assegnate aree di attesa per utenti o lead.

5. Fare clic su **Salva**.
6. Se si desidera modificare l'ordine in cui le divisioni sono visualizzate nell'elenco di selezione Divisioni, fare clic su **Ordina**, quindi utilizzare i pulsanti freccia per spostare le divisioni all'interno dell'elenco.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare o modificare divisioni:

- "Modifica tutti i dati"

VEDERE ANCHE:

Panoramica sulle divisioni

Impostazione delle divisioni

Trasferimento di più record tra le divisioni

Modifica della divisione predefinita degli utenti

## Trasferimento di più record tra le divisioni

Selezionare i gruppi o i record da spostare all'interno delle divisioni o tra di esse.

Per riassegnare le divisioni per più record alla volta, trasferire gruppi di account, lead o utenti tra le divisioni.

1. Da Imposta, immettere *Trasferisci globalmente divisioni* nella casella `Ricerca veloce`, quindi selezionare **Trasferisci globalmente divisioni**.
2. Selezionare i tipi di record che si desidera trasferire e fare clic su **Avanti**. Quando si modifica la divisione assegnata a un account, i record correlati, quali referenti e opportunità, vengono assegnati alla stessa divisione. Quando si modifica la divisione assegnata a un oggetto personalizzato, anche gli altri oggetti personalizzati che vi appartengono vengono trasferiti alla nuova divisione.
3. Selezionare i criteri di ricerca che i record devono soddisfare, quindi fare clic su **Avanti**.
4. Selezionare la divisione nella quale si desiderano trasferire i record.
5. Se si stanno trasferendo record utente, è possibile selezionare `Cambia divisione...` per trasferire anche i record utente nella nuova divisione.
6. Fare clic su **Trasferisci**. Al completamento del trasferimento si riceverà una notifica via email. Se vengono trasferiti 5.000 record o più, la richiesta verrà messa in attesa di elaborazione.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per trasferire globalmente i record:

- "Modifica tutti i dati"

VEDERE ANCHE:

Panoramica sulle divisioni

Impostazione delle divisioni

Creazione e modifica di divisioni

Modifica della divisione predefinita degli utenti

## Modifica della divisione predefinita degli utenti

Se è possibile gestire le impostazioni utente, è possibile modificare la divisione predefinita di un utente.

Se l'organizzazione utilizza le divisioni per segmentare i dati, a tutti gli utenti viene assegnata una divisione predefinita valida per i nuovi account, i lead e gli oggetti personalizzati. La divisione predefinita non impedisce agli utenti di visualizzare o creare record in altre divisioni. Se però il nuovo record è correlato a un record esistente, gli viene assegnata la stessa divisione del record esistente.

1. Da Imposta, immettere *Utenti* nella casella `Ricerca veloce`, quindi selezionare **Utenti**.
2. Fare clic sul nome, sull'alias o sul nome utente dell'utente di cui si desidera modificare la divisione predefinita.
3. Accanto al campo `Divisione predefinita`, fare clic su **Cambia**.
4. Selezionare una nuova divisione predefinita.
5. Selezionare un'azione da applicare ai record di cui l'utente è già titolare.
6. Fare clic su **Salva**.

Per modificare la propria divisione predefinita, saltare la fase 1 e accedere alle impostazioni personali. Immettere *Dettagli utente avanzati* nella casella `Ricerca veloce`, quindi

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per modificare la divisione predefinita di un utente:

- "Gestisci utenti"

selezionare **Dettagli utente avanzati**.Se non si ottiene alcun risultato, immettere `Informazioni personali` nella casella `Ricerca veloce`, quindi selezionare **Informazioni personali**.

VEDERE ANCHE:

Panoramica sulle divisioni

## Generazione di rapporti con le divisioni

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per limitare in rapporti in base alla divisione:

- "Limita per divisione"

Se l'organizzazione utilizza le divisioni per segmentare i dati è possibile personalizzare i rapporti per mostrare i record all'interno di divisioni specifiche.

Selezionare una delle opzioni seguenti dall'elenco a discesa Divisioni del rapporto.

- Una divisione specifica
- La divisione di lavoro corrente.
- Tutti i record di tutte le divisioni.

Nota: I rapporti che utilizzano filtri standard, ad esempio Casi personali o Account del team personale, mostrano i record di tutte le divisioni. Questi rapporti non si possono ulteriormente limitare a una divisione specifica.

VEDERE ANCHE:

Panoramica sulle divisioni

# Come posso interrompere il servizio?

Se il servizio non soddisfa le proprie esigenze, è possibile interromperlo. Gli utenti che non hanno pagamenti in arretrato possono richiedere di scaricare integralmente i dati presenti nel sistema. Per inviare direttamente la richiesta, contattare il reparto fatturazione dell'assistenza clienti di Salesforce.

# Autorizzazioni e impostazioni della Pagina iniziale di Lightning Experience

EDIZIONI

Disponibile nelle versioni: Lightning Experience

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Consentire ai propri utenti di accedere ai dettagli delle opportunità e ad altre autorizzazioni in modo che possano utilizzare al meglio la Pagina iniziale.

Non è possibile personalizzare il layout della pagina inziale, aggiungere componenti personalizzati o spostare gli elenchi correlati.

Per informazioni sull'abilitazione di Approfondimenti account, vedere "Impostazioni account" nella Guida di Salesforce.

Il grafico delle prestazioni e Trattative migliori visualizzano informazioni sulle opportunità relative al team di vendita di un utente, se è presente un team associato. In caso contrario, il grafico visualizza le opportunità di cui l'utente è titolare.

Per compilare il grafico delle prestazioni, Trattative migliori e l'Assistente, gli utenti devono disporre di quanto indicato di seguito.

**Tabella 1: Autorizzazioni richieste per le funzioni della Pagina iniziale**

| Autorizzazione o impostazione | Grafico delle prestazioni | Trattative migliori | Assistente |
|---|---|---|---|
| Accesso in lettura all'oggetto Opportunità e accesso in condivisione alle opportunità pertinenti | ✓ | ✓ | ✓ |
| Accesso in lettura al campo Ammontare dell'oggetto Opportunità | ✓ | ✓ | |
| Accesso in lettura al campo Probabilità dell'oggetto Opportunità | ✓ | | |
| Autorizzazione utente "Esegui rapporti" abilitata per gli utenti | ✓ | | |
| Opportunità chiuse o opportunità aperte con una probabilità superiore al 70% durante il trimestre corrente | ✓ | | |
| Accesso in lettura all'oggetto Lead e accesso in condivisione ai lead pertinenti | | | ✓ |

Nota: l'anno fiscale personalizzato non è supportato in Lightning Experience. Il grafico delle prestazioni visualizza soltanto le prestazioni di vendita del trimestre in corso.

# Gestione degli utenti

## Panoramica sulla gestione degli utenti

In Salesforce, ogni utente è identificato da un nome utente, una password e un profilo individuale. Insieme ad altre impostazioni, il profilo determina le attività che gli utenti possono eseguire, i dati che possono visualizzare e le operazioni possibili su questi dati.

A seconda della versione (Edition) Salesforce della propria organizzazione e delle funzioni aggiuntive acquistate, si hanno a disposizione licenze funzioni, ad esempio Marketing, Connect Offline e Sales Anywhere, che offrono agli utenti la possibilità di accedere a funzioni non incluse nelle loro licenze utente. A ciascun utente può essere assegnata una o più di queste licenze. Inoltre, è possibile impostare account per gli utenti esterni all'organizzazione e che necessitano di accedere a un gruppo limitato di campi e oggetti. Con le licenze utente è possibile anche concedere l'accesso al Portale Clienti, al portale partner o a Self-Service. Infine, con Salesforce a Salesforce, è possibile creare connessioni con cui condividere i record con altri utenti Salesforce esterni all'organizzazione.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Le opzioni di gestione degli utenti disponibili variano a seconda della versione di Salesforce utilizzata.

Nota: A partire dal rilascio Spring '12, il portale Self-Service non è disponibile per le nuove organizzazioni. Le organizzazioni esistenti continuano ad avere accesso al portale Self-Service.

In qualità di amministratore, è possibile eseguire operazioni di gestione degli utenti, come ad esempio creare e modificare utenti, reimpostare le password e creare account Google Apps. È inoltre possibile concedere autorizzazioni, creare e gestire altri tipi di utenti, creare campi personalizzati, impostare link personalizzati, eseguire rapporti sugli utenti e delegare le operazioni di amministrazione ad altri utenti.

VEDERE ANCHE:

Visualizzazione e gestione degli utenti

Panoramica sulle licenze

# Visualizzazione e gestione degli utenti

Per visualizzare e gestire gli utenti nell'organizzazione, da Imposta, immettere *Utenti* nella casella `Ricerca veloce`, quindi selezionare **Utenti**.

L'elenco utenti mostra tutti gli utenti dell'organizzazione, del portale partner e del Portale Clienti Salesforce. Dall'elenco utenti è possibile:

- Creare un utente.
- Creare più utenti.
- Reimpostare le password per gli utenti selezionati.
- Modificare un utente.
- Visualizzare la pagina dei dettagli di un utente facendo clic sul nome, l'alias o il nome utente.
- Visualizzare o modificare un profilo facendo clic sul nome del profilo.
- Se nell'organizzazione è abilitata Google Apps™, esportare gli utenti in Google e creare account di Google Appsfacendo clic su **Esporta in Google Apps**

Suggerimento: molte di queste operazioni possono essere eseguite dall'app mobile SalesforceA.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

I Portali Clienti e i portali partner non sono disponibili nella versione **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare gli elenchi utenti:

- "Visualizza impostazione e configurazione"

## Suggerimenti per la gestione degli utenti

- È possibile creare campi personalizzati per gli utenti e impostare link personalizzati da visualizzare nella pagina dei dettagli degli utenti. Per accedere a queste opzioni, accedere alle impostazioni di gestione degli oggetti per gli utenti.
- È possibile utilizzare la ricerca dall'intestazione laterale per cercare qualsiasi utente nell'organizzazione, indipendentemente dal suo stato. Tuttavia, quando si utilizza una finestra di dialogo di ricerca dai campi all'interno dei record, la ricerca restituisce solo gli utenti attivi. È possibile anche eseguire rapporti utenti nella scheda Rapporti.
- Per semplificare la gestione degli utenti nelle organizzazioni con un numero elevato di utenti, è possibile delegare aspetti dell'amministrazione utenti a utenti non amministratori.

Nota: non è possibile delegare funzioni amministrative correlate all'organizzazione agli utenti del portale partner o del Portale Clienti. Tuttavia, è possibile delegare alcune funzioni amministrative del portale agli utenti del portale.

VEDERE ANCHE:

Disattivazione (eliminazione) di utenti

Congelamento o scongelamento degli account utente

SalesforceA

## Linee guida per l'aggiunta di utenti

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Familiarizzare con le opzioni principali per l'aggiunta degli utenti. Imparare quali dati comunicare agli utenti in relazione alle password e agli accessi.

- Il *nome utente* deve essere univoco in tutte le organizzazioni Salesforce. Il nome utente deve essere sotto forma di indirizzo email, ad esempio giulia@salesforce.com. Tuttavia, l'indirizzo email effettivo nel nome utente non deve necessariamente essere funzionante. È *possibile* disporre degli stessi indirizzi email funzionanti associati al proprio account nelle varie organizzazioni, solo il *nome utente nel formato di un indirizzo email* deve rimanere univoco.
- Se il nome dell'utente contiene caratteri diversi da quelli latini, aggiungere la lingua in questione alle impostazioni di formato dell'email in Outlook (se le email vengono visualizzate in Outlook).
- Le password temporanee dei nuovi utenti scadono entro sei mesi ed è necessario modificarle la prima volta che si esegue l'accesso. Il link di accesso nel messaggio email si può utilizzare una sola volta. Un utente che segue il link senza impostare una password dovrà chiedere all'amministratore di reimpostare la sua password prima di poter accedere.
- È possibile trasformare una licenza Salesforce in una licenza Force.com, ma non è possibile trasformare una licenza Force.com in una licenza Salesforce.
- Non tutte le opzioni sono disponibili per tutti i tipi di licenze. Ad esempio, le opzioni `Utente marketing` e `Consenti previsioni` non sono disponibili per le licenze utente Force.com in quanto le schede Previsioni e Campagne non sono disponibili per gli utenti con una licenza Force.com. Le licenze utente Force.com non sono disponibili per le versioni Professional Edition, Group Edition e Contact Manager Edition.
- Nelle organizzazioni che utilizzano le versioni Performance Edition, Unlimited Edition, Enterprise Edition e Developer Edition, è possibile selezionare `Invia avvisi email Apex` per inviare un messaggio email all'utente quando un'applicazione che richiama Apex utilizza oltre la metà delle risorse specificate dai limiti del governor. Questa funzione può essere utilizzata durante lo sviluppo di Apex code per verificare la quantità di risorse utilizzate in fase di esecuzione.
- Le password temporanee dei nuovi utenti scadono entro sei mesi ed è necessario modificarle la prima volta che si esegue l'accesso. Il link di accesso nel messaggio email si può utilizzare una sola volta. Un utente che segue il link senza impostare una password dovrà chiedere all'amministratore di reimpostare la sua password prima di poter accedere.

VEDERE ANCHE:

Aggiunta di un singolo utente

## Aggiunta di un singolo utente

A seconda delle dimensioni dell'organizzazione o della procedura di orientamento per i nuovi assunti, è possibile scegliere di aggiungere un utente alla volta. Il numero massimo di utenti che è possibile aggiungere è determinato dalla versione (Edition) di Salesforce di cui si dispone.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per creare utenti:
- "Gestisci utenti interni"

1. Consultare le linee guida per l'aggiunta di utenti.
2. Da Imposta, immettere `Utenti` nella casella `Ricerca veloce`, quindi selezionare **Utenti**.
3. Fare clic su **Nuovo utente**.
4. Immettere il nome e l'indirizzo email dell'utente e un nome utente univoco sotto forma di un indirizzo email. Per impostazione predefinita, il nome utente è lo stesso dell'indirizzo email.

   Importante: Il *nome utente* deve essere univoco in tutte le organizzazioni Salesforce. Il nome utente deve essere sotto forma di indirizzo email, ad esempio giulia@salesforce.com. Tuttavia, l'indirizzo email effettivo nel nome utente non deve necessariamente essere funzionante. È *possibile* disporre degli stessi indirizzi email funzionanti associati al proprio account nelle varie organizzazioni, solo il *nome utente nel formato di un indirizzo email* deve rimanere univoco.

5. Nelle versioni Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition e Developer Edition, selezionare un `Ruolo`.
6. Selezionare una `licenza utente`. La licenza utente determina quali profili sono disponibili per l'utente.
7. Selezionare un profilo che specifica le autorizzazioni minime e le impostazioni di accesso dell'utente.
8. Se nell'organizzazione sono abilitate le approvazioni, è possibile definire le impostazioni responsabile approvazioni dell'utente, ad esempio responsabile approvazioni delegato o responsabile e le preferenze per la ricezione delle email con richiesta di approvazione.
9. Selezionare l'opzione `Genera nuova password e notifica utente immediatamente` per fare in modo che il nome di accesso dell'utente e la password temporanea vengano inviati in un messaggio email al nuovo utente.

VEDERE ANCHE:

Linee guida per l'aggiunta di utenti

Aggiunta di più utenti

Modifica degli utenti

Campi utente

Panoramica sulle licenze

## Aggiunta di più utenti

È possibile aggiungere rapidamente fino a 10 utenti all'organizzazione. Il numero massimo di utenti che è possibile aggiungere è determinato dalla versione di Salesforce in uso.

1. Da Imposta, immettere *Utenti* nella casella `Ricerca veloce`, quindi selezionare **Utenti**.
2. Fare clic su **Aggiungi più utenti**.
3. Se sono disponibili più tipi di licenza utente nell'organizzazione, selezionare quella da associare agli utenti che si prevede di creare. La licenza utente determina i profili disponibili.
4. Specificare le informazioni per ciascun utente.
5. Per inviare via email a ogni nuovo utente il nome di accesso e la password temporanea, selezionare **Genera password e avvisa l'utente tramite email**.
6. Fare clic su **Salva**.
7. Per specificare ulteriori dettagli relativi agli utenti creati con questo metodo, modificare i singoli utenti in funzione delle esigenze.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per creare utenti:
- "Gestisci utenti interni"

VEDERE ANCHE:

Aggiunta di un singolo utente
Modifica degli utenti
Campi utente
Panoramica sulle licenze

## Modifica degli utenti

Per modificare i dettagli dell'utente, ad esempio il profilo, il ruolo o le informazioni di contatto, modificare l'account dell'utente.

1. Da Imposta, digitare *Utenti* nella casella `Ricerca veloce` e quindi selezionare **Utenti**.
2. Fare clic su **Modifica** accanto al nome dell'utente.
3. Modificare le impostazioni in funzione delle esigenze.
4. Fare clic su **Salva**.

Suggerimento: questa e altre operazioni di amministrazione possono essere eseguite dall'app mobile SalesforceA.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per modificare gli utenti:
- "Gestisci utenti interni"

VEDERE ANCHE:

Campi utente
Considerazioni per la modifica degli utenti
Sblocco degli utenti
SalesforceA

## Considerazioni per la modifica degli utenti

Quando si modificano degli utenti, tenere presenti i seguenti comportamenti.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

**Nomi utente**

Il nome utente deve essere univoco in tutte le organizzazioni Salesforce. Deve utilizzare il formato di un indirizzo email (ad esempio xyz@abc.org), ma non è necessario che sia un indirizzo email reale. Sebbene gli utenti possano avere lo stesso indirizzo email nelle varie organizzazioni, i nomi utente devono essere univoci.

Se si modifica un nome utente, viene inviato un messaggio email di conferma contenente un link di accesso all'indirizzo associato all'account di quell'utente. Se un'organizzazione ha più server di accesso, talvolta dopo aver modificato un nome utente non si riesce subito a effettuare l'accesso. La replica della modifica su tutti i server può richiedere fino a 24 ore.

**Modifica degli indirizzi email**

Se l'opzione `Genera nuova password e notifica utente immediatamente` è disabilitata quando si modifica l'indirizzo email di un utente, Salesforce invia un messaggio di conferma all'indirizzo email immesso. Per rendere effettivo il nuovo indirizzo, gli utenti devono fare clic sul link contenuto nel messaggio. Tale processo è necessario per garantire la protezione del sistema.

**Informazioni personali**

Una volta eseguito l'accesso, gli utenti possono modificare le proprie informazioni personali.

**Condivisione utenti**

Se l'impostazione predefinita di tutta l'organizzazione per l'oggetto utente è Privato, gli utenti devono avere l'accesso in Lettura o Scrittura all'utente di destinazione per poter accedere alle informazioni su quell'utente.

**Nomi di dominio**

Gli utenti possono limitare i nomi di dominio degli indirizzi email degli utenti a un elenco di domini specifici. Qualsiasi tentativo di impostare un indirizzo email con un altro dominio causa un messaggio di errore. Per abilitare questa funzione nella propria organizzazione, contattare Salesforce.

VEDERE ANCHE:

Modifica degli utenti

## Sblocco degli utenti

Agli utenti che immettono troppe volte credenziali di accesso errate può venire bloccato l'accesso all'organizzazione. Sbloccare gli utenti per ripristinare l'accesso.

1. Da Imposta, immettere *Utenti* nella casella `Ricerca veloce`, quindi selezionare **Utenti**.
2. Selezionare l'utente bloccato.
3. Fare clic su **Sblocca**.

   Questo pulsante viene visualizzato solo quando un utente è bloccato.

Suggerimento: questa e altre operazioni di amministrazione possono essere eseguite dall'app mobile SalesforceA.

VEDERE ANCHE:

Modifica degli utenti

Impostazione dei criteri relativi alle password

SalesforceA

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per sbloccare gli utenti:
- "Gestisci utenti interni"

## Disattivazione (eliminazione) di utenti

Non è possibile eliminare un utente, ma è possibile disattivare un account in modo che un utente non possa più effettuare l'accesso a Salesforce.

1. Da Imposta, immettere *Utenti* nella casella `Ricerca veloce`, quindi selezionare **Utenti**.
2. Fare clic su **Modifica** accanto al nome dell'utente.
3. Deselezionare la casella di controllo `Attivo`, quindi fare clic su **Salva**.

Suggerimento: questa e altre operazioni di amministrazione possono essere eseguite dall'app mobile SalesforceA.

VEDERE ANCHE:

Considerazioni per la disattivazione degli utenti

Congelamento o scongelamento degli account utente

Trasferimento globale di record

SalesforceA

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per disattivare gli utenti:
- "Gestisci utenti interni"

## Considerazioni per la disattivazione degli utenti

Quando si disattivano degli utenti, tenere presenti i seguenti comportamenti.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

**Licenze utente e fatturazione**

Gli utenti disattivati non vengono conteggiati per le licenze utente disponibili nell'organizzazione. Tuttavia, la disattivazione di un utente non riduce il numero delle licenze fatturate per l'organizzazione. Per modificare la fatturazione è necessario cambiare il conteggio delle licenze dell'organizzazione.

**Utenti in campi personalizzati della gerarchia**

Non è possibile disattivare un utente selezionato in un campo gerarchia personalizzato, anche se si elimina il campo. Per disattivare un utente in un campo gerarchia personalizzato, è necessario prima eliminare e cancellare in modo definitivo il campo.

**Destinatari degli avvisi email di flusso di lavoro**

Non è possibile disattivare un utente se questo è l'unico destinatario di un avviso email di flusso di lavoro.

**Utenti amministratori del Portale Clienti**

Non è possibile disattivare un utente selezionato come `Amministratore` del Portale Clienti.

**Accesso ai record**

Gli utenti disattivati perdono l'accesso a tutti i record manualmente condivisi con essi oppure ai record condivisi con essi come membri del team. Anche gli utenti a un livello superiore nella gerarchia dei ruoli rispetto agli utenti disattivati perdono accesso a tali record. Tuttavia, è possibile trasferire i loro dati ad altri utenti e visualizzare i loro nomi nella pagina Utenti.

Nota: Se nell'organizzazione è abilitata l'eliminazione asincrona delle condivisioni obsolete (pilota), la rimozione delle condivisioni manuali e dei team viene eseguita durante gli orari di attività ridotta, tra le 18:00 e le 4:00, in base al fuso orario predefinito dell'organizzazione. Per i record di account, le condivisioni manuali e dei team vengono eliminate subito dopo la disattivazione degli utenti.

Gli utenti disattivati perdono immediatamente accesso ai record condivisi. Gli utenti a un livello superiore nella gerarchia dei ruoli mantengono l'accesso fino a che questo viene eliminato in modo asincrono. Se non si desidera che questa visibilità venga mantenuta, prima della disattivazione rimuovere l'accesso ai record concesso agli utenti disattivati.

**Chatter**

Se si disattivano degli utenti in un'organizzazione in cui è abilitato Chatter, tali utenti vengono rimossi dagli elenchi Stai seguendo e Chi segue. Se si riattivano gli utenti, i dati dell'abbonamento degli elenchi Stai seguendo e Chi segue vengono ripristinati.

Se si disattivano più utenti, i dati dell'abbonamento non vengono ripristinati per gli utenti che si seguono a vicenda. Ad esempio, se l'utente A segue l'utente B e l'utente B segue l'utente A, quando si disattivano gli utenti A e B i dati dei relativi abbonamenti reciproci vengono eliminati dagli elenchi Stai seguendo e Chi segue. Se in seguito l'utente A e l'utente B vengono riattivati, i relativi abbonamenti reciproci non vengono ripristinati.

**Campi `Creato da`**

Gli utenti inattivi possono essere elencati nei campi `Creato da` anche se non sono più attivi in un'organizzazione. Questo accade in quanto alcune operazioni di sistema creano record e attivano/disattivano le preferenze, agendo da utente amministratore arbitrario per completare l'operazione. Questo utente può essere attivo o inattivo.

**Account e opportunità di proprietà di utenti disattivati**

Gli utenti disattivati continuano a essere titolari delle opportunità e ad apparire nelle previsioni e nei territori. Quando gli utenti vengono disattivati, tutti i loro Ignora di previsioni opportunità e totali rettificati e gli Ignora di scelte responsabile nelle previsioni subordinate vengono congelati. Tuttavia, il responsabile di un utente disattivato può applicare Ignora di scelte responsabile alle previsioni di quell'utente. Gli importi di roll-up vengono mantenuti aggiornati, in modo che se un utente disattivato viene in seguito

riattivato, potrà riprendere a lavorare normalmente. Se l'opzione "Consenti previsioni" viene disabilitato per un utente disattivato, l'utente viene rimosso dai territori a cui è assegnato.

L'utente può creare e modificare record di account, opportunità e oggetti personalizzati di cui sono titolari utenti inattivi. Ad esempio, è possibile modificare il campo `Nome account` su un record opportunità di cui è titolare un utente inattivo. Per abilitare questa funzione, rivolgersi a Salesforce.

**Team opportunità e account**

Gli utenti disattivati vengono rimossi dai team opportunità e account predefiniti di altri utenti. I team predefiniti opportunità e account degli utenti disattivati non vengono rimossi.

**Team account**

Se un utente di un team account ha accesso in lettura/scrittura (**Accesso account**, **Accesso referenti**, **Accesso opportunità** e **Accesso casi**) e viene disattivato, nel momento in cui viene riattivato, per impostazione predefinita, il suo accesso sarà di sola lettura.

**Team opportunità**

Se si disattivano degli utenti in un'organizzazione in cui è abilitata la ripartizione delle opportunità, tali utenti non vengono rimossi da alcun team opportunità del quale gli sia stata assegnata una percentuale di ripartizione. Per rimuovere un utente da un team opportunità, è necessario prima riassegnare la percentuale di ripartizione.

**Amministratori utenti esterni delegati**

Quando disattiva un utente del portale, l'amministratore utente esterno delegato non ha la possibilità di rimuovere l'utente dai team di cui è membro.

VEDERE ANCHE:

Disattivazione (eliminazione) di utenti

## Congelamento o scongelamento degli account utente

Può accadere che non sia possibile disattivare immediatamente un account, ad esempio quando un utente è selezionato in un campo gerarchia personalizzato. Per impedire agli utenti di accedere all'organizzazione mentre si interviene per disattivarli, è possibile congelare gli account utente.

Si immagini che un utente abbia appena lasciato la società. Si desidera disattivare l'account, ma l'utente è selezionato in un campo gerarchia personalizzato. Poiché non è possibile disattivare immediatamente l'account, nel frattempo è possibile congelarlo.

Suggerimento: questa e altre operazioni di amministrazione possono essere eseguite dall'app mobile SalesforceA.

1. Da Imposta, immettere *Utenti* nella casella `Ricerca veloce`, quindi selezionare **Utenti**.
2. Fare clic sul nome utente dell'account che si desidera congelare.
3. Fare clic su **Congela** per bloccare l'accesso all'account o su **Scongela** per permettere nuovamente l'accesso all'account.

Nota: il congelamento degli account utente non rimette a disposizione dell'organizzazione le loro licenze utente. Per renderle disponibili, disattivare gli account.

VEDERE ANCHE:

Disattivazione (eliminazione) di utenti

SalesforceA

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per congelare o scongelare gli account utente:

- "Gestisci utenti"

## Limitazione dei domini di email degli utenti

È possibile definire una whitelist per limitare i domini di email ammessi nel campo `Email` di un utente.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

AUTORIZZAZIONI UTENTE

Per limitare i domini di email degli utenti:

- "Gestisci utenti"

1. Da Imposta, immettere *Domini di email consentiti* nella casella `Ricerca veloce`, quindi selezionare **Domini di email consentiti**.

   Nota: se questa pagina non è visualizzata, rivolgersi al rappresentante Salesforce per abilitarla.

2. Fare clic su **Nuovo dominio di email consentito**.
3. Immettere un `Dominio`.

   Si può immettere un dominio di primo livello come *sampledoc.org* o un sottodominio come *emea.sampledoc.org*.

4. Fare clic su **Salva**.

Queste operazioni si possono ripetere per aggiungere altri domini di email alla whitelist.

Dopo che alla whitelist sono stati aggiunti uno o più domini di email, il campo `Email` di ogni nuovo utente deve corrispondere a un dominio presente nella whitelist.

Non è necessario che il campo `Email` degli utenti esistenti sia conforme alla whitelist. Tuttavia, se si modifica un utente esistente, aggiornare il campo `Email` in modo che contenga un dominio di email presente nella whitelist.

Nota: la whitelist dei domini di email non è valida per gli utenti esterni all'organizzazione quali gli utenti dei portali, delle comunità o gli utenti esterni Chatter.

VEDERE ANCHE:

Aggiunta di un singolo utente
Aggiunta di più utenti
Modifica degli utenti

## Campi utente

I campi che compongono le pagine delle Informazioni personali e delle altre impostazioni personali agevolano la descrizione dell'utente.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

I campi disponibili variano secondo la versione (Edition) di Salesforce utilizzata.

La visibilità dei campi dipende dalle singole pagine visualizzate, dalle autorizzazioni dell'organizzazione e dalla versione in uso.

| Campo | Descrizione |
| --- | --- |
| `Modalità di accessibilità` | Se selezionato, consente di utilizzare un'interfaccia utente progettata per gli utenti non vedenti. |
| `Attivo` | Casella di controllo amministrativa che abilita e disabilita l'accesso degli utenti al servizio. |
| `Indirizzo` | Indirizzo postale dell'utente. Questo campo consente fino a 255 caratteri. |

| Campo | Descrizione |
| --- | --- |
| `Newsletter amministratore` | Consente di ricevere messaggi promozionali indirizzati all'amministratore da parte di Salesforce. Questo campo non è disponibile se l'organizzazione ha disabilitato la possibilità di scegliere se ricevere messaggi email da Salesforce. |
| `Alias` | Nome breve per identificare l'utente su pagine di elenco, rapporti e altre pagine che non possono contenere l'intero nome. Questo campo consente fino a otto caratteri. |
| `Consenti previsioni` | Indica se l'utente può utilizzare le previsioni personalizzabili. |
| `Token Api` | Indica se un token API è stato reimpostato. Se si verificano dei problemi, Salesforce utilizza questo campo per consentire la soluzione di problemi relativi ai token API. |
| `Call center` | Nome del call center a cui è assegnato l'utente. |
| `Checkout abilitato` | Indica se l'utente viene informato via email dell'attivazione del proprio account Checkout e della possibilità di accedervi.<br>L'abilitazione di questa opzione richiede l'autorizzazione "Gestisci fatturazione". |
| `Città` | Porzione dell'indirizzo dell'utente che indica la città. Questo campo consente fino a 40 caratteri. |
| `Tavolozza colori per daltonici sui grafici` | Indica se è stata abilitata l'opzione per impostare una tavolozza colori alternativa per i grafici. La tavolozza alternativa è stata ottimizzata per gli utenti daltonici. La tavolozza alternativa non viene utilizzata per i messaggi email con cruscotti digitali. |
| `Società` | Nome della società dove lavora l'utente. Questo campo consente fino a 40 caratteri. |
| `Referente` | Nome del referente associato se l'utente è un utente partner. |
| `Paese` | Porzione dell'indirizzo dell'utente che indica la nazione. La voce viene selezionata da un elenco di selezione di valori standard o inserita come testo. Se il campo è di testo, è consentito un massimo di 80 caratteri. |
| `Creato da` | Utente che ha creato l'utente incluse la data e l'ora di creazione. (Sola lettura) |
| `Valuta` | Valuta predefinita dell'utente per quote, previsioni e rapporti. Viene visualizzata solo nelle organizzazioni che utilizzano più valute. La valuta deve essere una delle valute attive dell'organizzazione. |
| `Link personalizzati` | Elenco dei link personalizzati per gli utenti, in base alle impostazioni del proprio amministratore. |
| `Tipo di utente Data.com` | Consente all'utente di trovare i record di referenti e lead di Data.com e di aggiungerli in Salesforce. Indica anche il tipo di utente Data.com. Gli utenti Data.com dispongono di un numero |

| Campo | Descrizione |
|---|---|
| | limitato di record di account, referenti e lead da aggiungere o esportare ogni mese e le aggiunte inutilizzate scadono alla fine di ogni mese. Gli utenti Data.com List dispongono di un numero limitato di record di account, referenti e lead da aggiungere o esportare ogni mese e le aggiunte inutilizzate scadono alla fine di ogni mese. Dopo che è stato esaurito il limite mensile, gli utenti List possono utilizzare aggiunte di record da un gruppo condiviso da tutti gli utenti List dell'organizzazione. Le aggiunte inutilizzate del gruppo scadono dopo un anno dall'acquisto. |
| `Codice ISO predefinito valuta` | Impostazione predefinita della valuta dell'utente per i nuovi record. Disponibile solo per le organizzazioni che utilizzano più valute. |
| `Divisione predefinita` | Divisione applicata, per impostazione predefinita, a tutti i nuovi account e lead creati dall'utente, a meno che l'utente non abbia impostato in modo esplicito una divisione diversa. Quando si creano record correlati a un account o a un altro record che dispone già di una divisione, il nuovo record viene assegnato alla divisione del record esistente. La divisione predefinita non viene utilizzata.<br>Questa impostazione non impedisce all'utente di visualizzare o creare record in altre divisioni. Gli utenti possono modificare la divisione predefinita in qualsiasi momento, impostando una divisione di lavoro.<br>Disponibile solo nelle organizzazioni che utilizzano le divisioni per segmentare i propri dati. |
| `Responsabile approvazioni delegato` | Campo di ricerca utente utilizzato per selezionare un responsabile delle approvazioni delegato per le richieste di approvazione. In base alle impostazioni del processo di approvazione, questo utente può inoltre approvare le richieste di approvazione per l'utente. |
| `Reparto` | Gruppo per cui lavora l'utente, ad esempio Assistenza clienti. Questo campo consente fino a 80 caratteri. |
| `Modalità sviluppo` | Consente la modalità sviluppo per la creazione e la modifica delle pagine Visualforce.<br>Questo campo è visibile solo per le organizzazioni per cui è abilitato Visualforce. |
| `Disabilita abbonamento automatico ai feed` | Disabilita gli abbonamenti automatici ai feed per i record di proprietà di un utente. Disponibile solo per le organizzazioni in cui è abilitato Chatter. |
| `Divisione` | Divisione della società a cui appartiene l'utente, ad esempio Gruppo vendite PC. Questo campo consente fino a 40 caratteri. |
| `Indirizzo email` | Indirizzo email dell'utente. Deve essere un indirizzo email valido nel formato: jsmith@acme.com. Questo campo consente fino a 80 caratteri. |

| Campo | Descrizione |
|---|---|
| Codifica email | Set di caratteri e codifica per i messaggi in uscita inviati dall'interno di Salesforce. Gli utenti di lingua inglese usano ISO-8859-1, che rappresenta tutti i caratteri latini. UTF-8 (Unicode) rappresenta i caratteri di tutte le lingue, tuttavia non è supportata da alcuni software di email meno recenti. Shift_JIS, EUC-JP e ISO-2022-JP sono utili per gli utenti giapponesi. |
| Numero dipendente | Numero di identificazione per un utente. |
| Fine giornata | Ora in cui l'utente normalmente smette di lavorare. Viene utilizzata per definire gli orari visualizzati nel calendario dell'utente. |
| Fax | Numero di fax dell'utente. |
| ID federazione | Valore utilizzato per identificare un utente per il Single-Sign-On con autenticazione federata. |
| Nome | Nome dell'utente, come viene visualizzato nella pagina di modifica utente. Questo campo consente fino a 40 caratteri. |
| Utente Force.com Flow | Concede la possibilità di eseguire i flussi. Disponibile nelle versioni Developer Edition (con limitazioni), Enterprise Edition, Unlimited Edition e Performance Edition.<br>L'abilitazione di questa opzione richiede l'autorizzazione "Gestisci flusso Force.com".<br>Se l'utente dispone dell'autorizzazione "Esegui flussi", non abilitare questo campo. |
| Menu di accesso rapido Force.com | Abilita il menu di accesso rapido Force.com che compare nella visualizzazione elenco degli oggetti e nelle pagine dei dettagli dei record. Il menu offre scelte rapide per le funzioni di personalizzazione di applicazioni e oggetti. |
| Valuta informazioni | Valuta predefinita per tutti i campi di importi in valuta nel record dell'utente. Disponibile solo per le organizzazioni che utilizzano più valute. |
| Utente Knowledge | Concede l'accesso a Salesforce Knowledge. L'accesso alla scheda Gestione articoli o alla scheda Articoli è determinato dal profilo dell'utente. Disponibile nelle versioni Professional Edition, Enterprise Edition, Unlimited Edition e Performance Edition. |
| Lingua | Lingua principale dell'utente. Tutto il testo e la Guida in linea vengono visualizzati in questa lingua. Nelle organizzazioni Professional Edition, Enterprise Edition, Unlimited Edition e Performance Edition, l'impostazione Lingua di un singolo utente ha la precedenza sulla Lingua predefinita dell'organizzazione. |

| Campo | Descrizione |
| --- | --- |
| | Non è disponibile nelle versioni Personal Edition, Contact Manager o Group Edition™. La `Lingua di visualizzazione` dell'organizzazione è valida per tutti gli utenti. |
| `Ultimo accesso` | Data e ora dell'ultimo accesso effettuato dall'utente. Il valore viene aggiornato quando sono trascorsi 60 secondi dall'ultimo accesso dell'utente. (Sola lettura) |
| `Cognome` | Cognome dell'utente, come viene visualizzato nella pagina di modifica utente. Questo campo consente fino a 80 caratteri. |
| `Ultima modifica o ultimo ripristino della password` | Data e ora dell'ultima modifica o dell'ultimo ripristino della password di questo utente. Questo campo di sola lettura è visualizzato solo per gli utenti con autorizzazione "Gestisci utenti". |
| `Impostazioni internazionali` | Paese o area geografica in cui risiede l'utente.<br><br>Le `Impostazioni internazionali` determinano il formato dei campi data, data/ora, numerici e il calendario. Ad esempio, le date nelle impostazioni internazionali Inglese (Stati Uniti) vengono visualizzate nel formato 06/30/2000, mentre nelle impostazioni internazionali Inglese (Regno Unito) vengono visualizzate nel formato 30/06/2000. Nelle impostazioni internazionali Inglese (Stati Uniti) l'ora viene visualizzata utilizzando il formato 12 ore con i suffissi AM e PM (ad esempio, 2:00 PM), mentre nelle impostazioni internazionali Inglese (Regno Unito) viene visualizzata nel formato 24 ore (ad esempio, 14:00).<br><br>Le `Impostazioni internazionali` inoltre determinano l'ordine di visualizzazione di nome e cognome nei campi `Nome` relativi a utenti, lead e referenti. Ad esempio, Bob Johnson nelle impostazioni internazionali Inglese (Stati Uniti) viene visualizzato come Bob Johnson, mentre nelle impostazioni internazionali Cinese (Cina) appare come Johnson Bob.<br><br>Per gli utenti della versione Personal Edition, le impostazioni internazionali si configurano a livello di organizzazione (da Imposta, immettere *`Informazioni sulla società`* nella casella `Ricerca veloce`, quindi selezionare **Informazioni sulla società**). Per tutti gli altri utenti, le impostazioni internazionali personali definite nella pagina delle informazioni personali hanno la precedenza su quelle impostate per l'organizzazione. |
| `Fai della pagina Imposta la mia landing page predefinita` | Se l'opzione è attivata, al momento dell'accesso gli utenti visualizzano la pagina Imposta. |
| `Responsabile` | Campo di ricerca utilizzato per selezionare il responsabile dell'utente. Questo campo:<br><br>• Stabilisce un rapporto gerarchico per impedire la selezione di un utente che direttamente o indirettamente riferisce a se stesso. |

| Campo | Descrizione |
| --- | --- |
| | • Consente a Chatter di consigliare le persone e i record da seguire in base alla struttura di riferimento dell'organizzazione.<br><br>Questo campo è particolarmente utile per la creazione di regole di flusso di lavoro e processi di approvazione gerarchici poiché evita di creare ulteriori campi gerarchici.<br><br>Nota: A differenza di altri campi gerarchici, è possibile disattivare gli utenti a cui fa riferimento il campo `Responsabile`. |
| `Utente Marketing` | Se abilitato, l'utente può creare, modificare ed eliminare le campagne, configurare impostazioni avanzate delle campagne, importare lead e aggiornare la cronologia delle campagne tramite le procedure guidate di importazione dei membri. Disponibile nelle versioni Professional Edition, Enterprise Edition, Unlimited Edition e Performance Edition.<br><br>Per utilizzare le importazioni guidate delle campagne, gli Utenti Marketing devono inoltre disporre del profilo Utente marketing (o delle autorizzazioni "Importa lead" e "Modifica" per le campagne nelle organizzazioni Enterprise Edition, Unlimited Edition e Performance Edition).<br><br>Se questa opzione non è selezionata, l'utente può visualizzare solo le campagne e l'impostazione avanzata delle campagne, modificare la cronologia delle campagne per un solo lead o referente ed eseguire rapporti campagna. |
| `Secondo nome` | Secondo nome dell'utente, come viene visualizzato nella pagina di modifica utente. Questo campo consente fino a 40 caratteri.<br><br>Nota: Per abilitare questo campo, contattare l'Assistenza clienti di Salesforce. Poi, da Imposta, immettere *`Interfaccia utente`* nella casella `Ricerca veloce`, quindi selezionare **Interfaccia utente**. A questo punto, selezionare **Abilitazione dei suffissi dei nomi per i nomi di persona**. |
| `Cellulare` | Numero del telefono cellulare. Questo campo consente fino a 40 caratteri.<br><br>Questo numero viene utilizzato per la conferma dell'identità basata su SMS. Gli amministratori abilitano la conferma di identità basata su SMS da Imposta, immettendo *`Impostazioni di sessione`* nella casella `Ricerca veloce`, quindi selezionando **Impostazioni di sessione** e infine selezionando l'opzione **Abilita il metodo SMS di conferma dell'identità**.<br><br>Una volta abilitato il metodo di conferma dell'identità basato su SMS, agli utenti che non includono nel proprio profilo un numero di cellulare verificato verrà richiesto dopo l'accesso di registrarsi |

| Campo | Descrizione |
| --- | --- |
| | per la verifica via cellulare. Questo procedimento è valido per gli utenti privi di numero di cellulare. Gli utenti possono eseguire una tra le operazioni elencate di seguito.<br>• Immettere un numero di telefono cellulare e farlo verificare con un messaggio di testo contenente un codice di verifica.<br>• Non immettere subito il numero di cellulare e visualizzare di nuovo la richiesta all'accesso successivo.<br>• Ignorare la verifica via cellulare. Gli utenti che selezionano questa azione possono registrare un numero di cellulare nelle informazioni personali in un secondo momento. Gli utenti con licenza Chatter Free e Chatter External che selezionano questa azione dovranno ricorrere all'amministratore per impostare il numero di cellulare.<br>Una volta verificato il numero di cellulare di un utente, Salesforce lo usa per autenticare l'utente, quando necessario. Ad esempio, viene effettuata una verifica quando un utente accede da un indirizzo IP sconosciuto.<br>Gli amministratori possono inoltre immettere i numeri di cellulare degli utenti e verificarli preventivamente. Se l'opzione **Abilita il metodo SMS di conferma dell'identità** è abilitata quando un amministratore immette il numero di cellulare di un utente o quando un numero di cellulare viene impostato da un'API utilizzando l'oggetto `Utente`, il numero di cellulare viene considerato verificato. Se l'opzione **Abilita il metodo SMS di conferma dell'identità** non è abilitata, il nuovo numero di telefono cellulare non è considerato verificato. |
| `Configurazione mobile` | Configurazione mobile assegnata all'utente. Se non è specificata alcuna configurazione mobile, nel campo viene inserita per impostazione predefinita la configurazione mobile assegnata al profilo dell'utente.<br>Questo campo è visibile per le organizzazioni che utilizzano Salesforce per gestire le configurazioni mobili. |
| `Utente mobile` | Assegna all'utente una licenza Salesforce Classic mobile, consentendogli di accedere all'app Salesforce Classic mobile. Il numero dei record utente abilitato da questa casella di controllo non può superare il numero totale di licenze mobili dell'organizzazione. Disponibile nelle versioni Professional Edition, Enterprise Edition, Unlimited Edition e Performance Edition.<br>L'opzione **Utente mobile** è abilitata per impostazione predefinita per gli utenti delle versioni Unlimited Edition, Performance Edition e Developer Edition. Per evitare che gli utenti attivino l'app Salesforce Classic mobile sui loro dispositivi mobili prima che |

| Campo | Descrizione |
| --- | --- |
| | l'organizzazione sia pronta a implementarla, disabilitare l'opzione per tutti gli utenti.<br>Se gli utenti hanno già attivato l'account Salesforce Classic mobile e si deseleziona l'opzione **Utente mobile**, la licenza mobile dell'utente viene revocata. Alla successiva sincronizzazione del dispositivo dell'utente con Salesforce, tutti i dati di Salesforce vengono eliminati dal dispositivo che non viene più associato all'utente.<br>Nota: la casella di controllo `Utente mobile` non è valida per la versione gratuita di Salesforce Classic mobile perché gli utenti di questa app possono accedere a Salesforce dal loro dispositivo senza una licenza mobile. |
| `Modificato da` | Utente che ha modificato per ultimo i campi utente, incluse la data e l'ora della modifica. (Sola lettura) |
| `Limite mensile referenti e lead` | Se il `Tipo di utente Data.com` è Utente Data.com, numero di record di referenti e lead Data.com che l'utente può aggiungere ogni mese.<br>Il numero predefinito di record per ogni licenza è 300, ma è possibile assegnarne di più o di meno a seconda dei limiti stabiliti per l'organizzazione. |
| `Nome` | Nome, secondo nome (beta), cognome e suffisso (beta) combinati dell'utente, come visualizzati nella pagina dei dettagli dell'utente. |
| `Newsletter` | Consente di ricevere messaggi promozionali destinati all'utente da parte di Salesforce. Questo campo non è disponibile se l'organizzazione ha disabilitato la possibilità di scegliere se ricevere messaggi email da Salesforce. |
| `Nickname` | Il nickname è il nome utilizzato per identificare l'utente in una comunità. Sono consentiti al massimo 40 caratteri alfanumerici. Gli utenti standard possono modificare questo campo. |
| `Utente Offline` | Casella di controllo amministrativa che concede all'utente l'accesso a Connect Offline. Disponibile nelle versioni Professional Edition, Enterprise Edition, Unlimited Edition e Performance Edition. |
| `Super utente partner` | Indica se un utente del Portale Partner è un super utente. |
| `Telefono` | Numero di telefono dell'utente. Questo campo consente fino a 40 caratteri. |
| `Profilo` | Campo amministrativo che specifica le autorizzazioni di livello base dell'utente per l'esecuzione di diverse funzioni dell'applicazione. È possibile assegnare a un utente più autorizzazioni utilizzando gli insiemi di autorizzazioni. |

| Campo | Descrizione |
|---|---|
| `Ricevi messaggi email con richiesta di approvazione` | Preferenza per la ricezione di messaggi email con richieste di approvazione.<br><br>Questa preferenza determina anche se l'utente riceverà le notifiche delle richieste di approvazione in Salesforce1. |
| `Ricevi avvisi di Salesforce CRM Content come rapporto quotidiano` | Specifica che gli utenti non del portale con licenza `Utente Salesforce CRM Content` e abbonamento Salesforce CRM Content riceveranno un riepilogo email giornaliero se si verificano attività connesse a contenuti, librerie, tag o autori a cui si riferisce l'abbonamento. Per ricevere il messaggio email, è necessario selezionare anche l'opzione `Ricevi avvisi via email di Salesforce CRM Content` Gli utenti di portale non necessitano della licenza `Utente Salesforce CRM Content`. È sufficiente che dispongano dell'autorizzazione utente `Visualizza contenuto nei portali`. |
| `Ricevi avvisi tramite email di Salesforce CRM Content` | Specifica che gli utenti non del portale con licenza `Utente Salesforce CRM Content` e abbonamento Salesforce CRM Content riceveranno notifiche email se si verificano attività connesse a contenuti, librerie, tag o autori a cui si riferisce l'abbonamento. Per ricevere avvisi via email in tempo reale, selezionare questa opzione e non selezionare `Ricevi avvisi di Salesforce CRM Content come rapporto quotidiano`. Gli utenti del portale non necessitano della licenza `Utente Salesforce CRM Content`. È sufficiente che dispongano dell'autorizzazione utente `Visualizza contenuto nei portali`. |
| `Ruolo` | Campo amministrativo che specifica la posizione dell'utente all'interno di un'organizzazione, ad esempio Responsabile assistenza area occidentale. I ruoli vengono selezionati da un elenco di selezione dei ruoli disponibili, che può essere modificato da un amministratore.<br><br>Non è disponibile nelle versioni Personal Edition, Contact Manager o Group Edition. |
| `Utente Salesforce CRM Content` | Indica se un utente può utilizzare Salesforce CRM Content. Disponibile nelle versioni Professional Edition, Enterprise Edition, Unlimited Edition e Performance Edition. |
| `Utente Salesforce1` | Attiva il reindirizzamento automatico all'app browser mobile Salesforce1 quando un utente accede a Salesforce da un browser Web mobile supportato. È necessario che per l'organizzazione sia abilitata l'app browser mobile Salesforce1. |
| `Autoregistrato tramite il Portale Clienti` | Se abilitata, specifica che l'utente è stato creato tramite autoregistrazione a un Portale clienti. Disponibile nelle versioni Enterprise Edition, Unlimited Edition e Performance Edition. |

| Campo | Descrizione |
| --- | --- |
| `Invia avvisi tramite email Apex` | Specifica che gli utenti riceveranno una notifica email ogni volta che eseguono uno script Apex che supera di più del 50% i limiti del governor.<br><br>Disponibile solo nelle versioni Developer Edition, Enterprise Edition, Unlimited Edition e Performance Edition. |
| `Mostra stato visualizzazione in modalità sviluppo` | Abilita la scheda Stato visualizzazione nel piè di pagina della modalità di sviluppo per le pagine Visualforce.<br><br>Questo campo è visibile solo per le organizzazioni che hanno abilitato Visualforce e selezionato `Modalità sviluppo`. |
| `Utente Site.com Contributor` | Assegna all'utente una licenza Site.com Contributor, concedendogli accesso limitato a Site.com Studio. Gli utenti con licenza Contributor possono utilizzare Site.com Studio solo per modificare il contenuto del sito.<br><br>Il numero di record utente con questa casella di controllo abilitata non può superare il numero totale di licenze Site.com Contributor dell'organizzazione.<br><br>Disponibile nelle versioni Developer Edition, Enterprise Edition, Unlimited Edition e Performance Edition, solo se Site.com è abilitato per l'organizzazione. |
| `Utente Site.com Publisher` | Assegna una licenza Site.com Publisher all'utente, concedendogli accesso completo a Site.com Studio. Gli utenti con licenza Publisher possono creare siti Web e definirne gli stili, controllare il layout e il funzionamento delle pagine e degli elementi di pagina, aggiungere e modificare i contenuti.<br><br>Il numero di record utente con questa casella di controllo abilitata non può superare il numero totale di licenze Site.com Publisher dell'organizzazione.<br><br>Disponibile nelle versioni Developer Edition, Enterprise Edition, Unlimited Edition e Performance Edition, solo se Site.com è abilitato per l'organizzazione. |
| `Inizio giornata` | Ora in cui l'utente normalmente inizia a lavorare. Viene utilizzata per definire gli orari visualizzati nel calendario dell'utente. |
| `Stato/Provincia` | Porzione dell'indirizzo dell'utente che indica lo stato o la provincia. La voce viene selezionata da un elenco di selezione di valori standard o inserita come testo. Se il campo è di testo, è consentito un massimo di 80 caratteri. |
| `Suffisso` | Suffisso del nome dell'utente, come viene visualizzato nella pagina di modifica utente. Questo campo consente fino a 40 caratteri.<br><br>Nota: Per abilitare questo campo, contattare l'Assistenza clienti di Salesforce. Poi, da Imposta, immettere |

| Campo | Descrizione |
| --- | --- |
| | `Interfaccia utente` nella casella `Ricerca veloce`, quindi selezionare **Interfaccia utente**. A questo punto, selezionare `Abilitazione dei suffissi dei nomi per i nomi di persona`. |
| `Fuso orario` | Fuso orario principale in cui l'utente lavora. |
| `Token basato sul tempo` | Quando viene aggiunto, si può utilizzare per confermare l'identità dell'utente quando è necessario, ad esempio in caso di accesso da un indirizzo IP sconosciuto.<br>Se l'utente dispone dell'autorizzazione "Autenticazione a due fattori per gli accessi interfaccia utente", gli viene richiesto di immettere il token durante l'accesso a Salesforce tramite l'interfaccia utente.<br>Se l'utente dispone dell'autorizzazione "Autenticazione a due fattori per gli accessi API" e aggiunge un token basato sul tempo, per accedere al servizio dovrà immettere questo token anziché il token di sicurezza standard. |
| `Qualifica` | Qualifica professionale dell'utente. Questo campo consente fino a 80 caratteri. |
| `Spazio utilizzato` | Quantità di spazio di memoria sul disco utilizzata dall'utente. |
| `Licenza utente` | Indica il tipo di licenza dell'utente. |
| `Nome utente` | Campo amministrativo che definisce l'accesso dell'utente. Questo campo consente fino a 80 caratteri. |
| `CAP` | Porzione dell'indirizzo dell'utente che indica il codice postale. Questo campo consente fino a 20 caratteri. |

VEDERE ANCHE:

Visualizzazione e gestione degli utenti

Panoramica sulle licenze utente

Visualizzazione delle licenze funzioni dell'organizzazione

Limitazione dei domini di email degli utenti

# Panoramica sulle licenze

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

I requisiti relativi alla versione (Edition) variano per ciascun utente, insieme di autorizzazioni e tipo di licenza funzioni.

Per abilitare funzionalità di Salesforce specifiche per gli utenti è necessario scegliere una licenza utente per ciascun utente. Per abilitare ulteriori funzionalità è possibile assegnare agli utenti delle licenze insieme di autorizzazioni e delle licenze funzioni o acquistare diritti basati sull'utilizzo per l'organizzazione.

Funzioni specifiche di Salesforce richiedono autorizzazioni specifiche. Ad esempio, per visualizzare i casi, un utente deve avere l'autorizzazione "Lettura" per i casi. Tuttavia, non è possibile assegnare autorizzazioni a tutti gli utenti indifferentemente. Come le funzioni che abilita, ogni autorizzazione ha dei requisiti specifici. Per assegnare una determinata autorizzazione a un utente, la o le licenze dell'utente devono supportare l'autorizzazione. Una singola autorizzazione può essere supportata da più di una licenza.

Le autorizzazioni sono come dei lucchetti, e le licenze sono i mazzi di chiavi. Per poter assegnare agli utenti un'autorizzazione specifica, gli utenti devono disporre di una licenza che contenga la chiave per sbloccare quell'autorizzazione. Anche se ogni utente deve disporre di una sola licenza utente, è possibile assegnare una o più licenze insieme di autorizzazioni o licenze funzioni per sbloccare progressivamente altre autorizzazioni.

Per continuare con lo stesso esempio, la licenza utente Salesforce contiene la chiave per sbloccare l'autorizzazione "Lettura" per i casi, ma la licenza utente Force.com — App Subscription non la contiene. Se si tenta di assegnare questa autorizzazione a un utente Force.com — App Subscription, si riceve un messaggio di errore. Tuttavia, se a quell'utente Force.com — App Subscription è stata assegnata anche una licenza insieme di autorizzazioni Company Community per Force.com, è possibile assegnargli l'autorizzazione "Lettura" per i casi.

Salesforce dispone dei seguenti tipi di licenze e di diritti basati sull'utilizzo.

IN QUESTA SEZIONE:

## Panoramica sulle licenze utente

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

I requisiti relativi alla versione (Edition) variano per ogni tipo di licenza utente.

Una licenza utente determina la base delle funzionalità a cui l'utente può accedere. Ogni utente deve avere esattamente una sola licenza utente. Le autorizzazioni utente per l'accesso ai dati si assegnano mediante un profilo e, se necessario, uno o più insiemi di autorizzazioni.

Esempio: Ad esempio, se si assegna una licenza utente Force.com al dipendente A e una licenza utente Salesforce al dipendente B, è possibile concedere l'accesso in "Lettura" ai casi solo al dipendente B. La licenza utente del dipendente A non supporta autorizzazioni per oggetti personalizzati che non siano account e referenti.

Salesforce offre i seguenti tipi di licenze.

- Licenze utente standard
- Licenze utente Chatter
- Licenze utente comunità
- Licenze utente per il Portale Service Cloud
- Licenze utente Siti e Site.com
- Licenze utente Sito Web autenticato

Nota: se l'azienda ha acquistato licenze utente personalizzate per tipi di funzionalità diversi, è possibile che siano elencati altri tipi di licenze. L'organizzazione può inoltre avere altre licenze che sono ancora supportate ma non più acquistabili. Per ulteriori informazioni, contattare Salesforce.

I seguenti tipi di licenze sono disponibili solo per le organizzazioni che attualmente utilizzano un Portale Clienti o un Portale partner. Se non si dispone di un Portale Clienti o di un Portale partner ma si desidera condividere facilmente le informazioni con i propri clienti, vedere Licenze utente comunità a pagina 162.

- Licenze utente del Portale Clienti
- Licenze utente del Portale Clienti — Amministrazione aziendale
- Licenze utente Portale partner

IN QUESTA SEZIONE:

Licenze utente Sito Web autenticato

Gli utenti del Portale piattaforma dispongono di licenza Sito Web autenticato, che è stata creata appositamente per l'uso con Force.com Sites. Fornisce agli utenti denominati dei siti un numero illimitato di accessi al Portale Piattaforma per accedere alle informazioni di assistenza clienti.

VEDERE ANCHE:

Visualizzazione e gestione degli utenti

Come trovare informazioni sulla società

## Visualizzazione delle licenze utente dell'organizzazione

Visualizzare le licenze utente acquistate dall'organizzazione per vedere quali sono disponibili per l'assegnazione agli utenti.

1. Da Imposta, immettere *Informazioni sulla società* nella casella Ricerca veloce, quindi selezionare **Informazioni sulla società**.
2. Consultare l'elenco correlato Licenze utente.

Per informazioni sull'acquisto di licenze utente aggiuntive, vedere Acquisto di più licenze per gli utenti a pagina 124 o rivolgersi all'Assistenza clienti di Salesforce.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: Tutte le versioni

AUTORIZZAZIONI UTENTE

Per visualizzare le licenze utente:

- "Visualizza impostazione e configurazione"

## Licenze utente standard

Informazioni sulle licenze utente standard che si possono ottenere per l'organizzazione, ad esempio i tipi di licenza utente Salesforce e Force.com.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

I requisiti relativi alla versione (Edition) variano per ogni tipo di licenza utente.

| Tipo di licenza | Descrizione | Disponibile in |
| --- | --- | --- |
| Salesforce | Ideata per gli utenti che richiedono l'accesso completo alle applicazioni standard CRM e Force.com AppExchange. Gli utenti dotati di questa licenza utente dispongono dell'accesso a qualsiasi applicazione standard o personalizzata.<br><br>Ogni licenza fornisce ulteriore memoria per gli utenti delle versioni Enterprise Edition, Unlimited Edition e Performance Edition. | Tutte le versioni |
| Utente Knowledge Only | Ideata per gli utenti che hanno bisogno di accedere solo all'applicazione Salesforce Knowledge. Questa licenza consente di accedere a oggetti personalizzati, a schede personalizzate e alle seguenti schede standard.<br>• Articoli<br>• Gestione degli articoli<br>• Chatter<br>• File<br>• Pagina iniziale<br>• Profilo<br>• Rapporti<br>• Oggetti personalizzati<br>• Schede personalizzate | **Enterprise Edition**, **Unlimited Edition** e **Performance Edition** |

| Tipo di licenza | Descrizione | Disponibile in |
|---|---|---|
| | La licenza Utente Knowledge Only include un profilo Knowledge Only che consente di accedere alla scheda Articoli. Per visualizzare e utilizzare la scheda Gestione articoli, l'utente deve disporre dell'autorizzazione "Gestisci articoli". | |
| `Identity` | Consente agli utenti l'accesso alle funzioni di Salesforce Identity. Salesforce Identity collega gli utenti Salesforce ad applicazioni e servizi esterni consentendo agli amministratori di controllare le procedure di autenticazione e autorizzazione di tali utenti.<br>Per ulteriori informazioni, vedere la *Salesforce Identity Implementation Guide*. | **Enterprise Edition**, **Unlimited Edition**, **Performance Edition** e **Developer Edition**<br>Per ogni nuova organizzazione **Developer Edition** sono incluse dieci licenze utente Identity gratuite. |
| `External Identity` | Consente agli utenti esterni all'organizzazione (ad esempio, ai non dipendenti) di utilizzare le funzioni di Identity. Memorizza e gestisce questi utenti, ne sceglie le modalità di autenticazione (nome utente/password o accesso sociale con Single Sign-On tramite Facebook, Google+, LinkedIn e altri) e consente l'auto registrazione. | **Enterprise Edition**, **Unlimited Edition**, **Performance Edition** e **Developer Edition**<br>Per ogni nuova organizzazione **Developer Edition** sono incluse cinque licenze utente External Identity gratuite. |
| `Utente Solo Work.com` | Progettata per gli utenti che non dispongono di una licenza Salesforce e devono poter accedere a Work.com.<br>Nota: affinché tutte le funzioni di Work.com funzionino correttamente è necessario abilitare Chatter. | **Professional Edition**, **Enterprise Edition**, **Unlimited Edition**, **Performance Edition** e **Developer Edition** |

## Tipi di licenze utente Force.com

| Tipo di licenza | Descrizione | Disponibile in |
|---|---|---|
| `Salesforce Platform` | Ideata per gli utenti che hanno bisogno di accedere alle applicazioni personalizzate ma non alle funzionalità CRM standard. Gli utenti dotati di questa licenza utente hanno diritto di utilizzare le applicazioni personalizzate sviluppate nell'organizzazione o installate da Force.com AppExchange. Gli utenti possono inoltre utilizzare funzionalità essenziali della piattaforma come account, referenti, rapporti, cruscotti digitali, documenti e schede personalizzate. Non hanno tuttavia diritto ad alcune autorizzazioni utente e applicazioni standard, tra cui schede e oggetti standard come previsioni e opportunità. Gli utenti dotati di questa licenza possono utilizzare anche Connect Offline.<br>Nota: gli utenti che dispongono di questa licenza possono visualizzare i cruscotti digitali soltanto se anche l'utente in esecuzione dispone della stessa licenza. | **Enterprise Edition**, **Unlimited Edition**, **Performance Edition** e **Developer Edition** |

| Tipo di licenza | Descrizione | Disponibile in |
|---|---|---|
| | Gli utenti con licenza utente Salesforce Platform possono accedere a tutte le applicazioni personalizzate nell'organizzazione.<br><br>Ogni licenza fornisce ulteriore memoria per gli utenti delle versioni Enterprise Edition, Unlimited Edition e Performance Edition. | |
| `Force.com - One App` | Nota: questa licenza non è disponibile per i nuovi clienti.<br><br>Ideata per gli utenti che hanno bisogno di accedere a una applicazione personalizzata ma non alle funzionalità CRM standard. Gli utenti Force.com - One App hanno diritto agli stessi privilegi degli utenti Salesforce Platform, ma in più dispongono dell'accesso a un numero illimitato di schede personalizzate. Tuttavia, sono limitati all'uso di un'applicazione personalizzata, definita come un massimo di 10 oggetti personalizzati, e hanno un accesso di sola lettura agli oggetti Account e Referenti.<br><br>Nota: gli utenti che dispongono di questa licenza possono visualizzare i cruscotti digitali soltanto se anche l'utente in esecuzione dispone della stessa licenza.<br><br>Ciascuna licenza fornisce 20 MB di memoria dati in più e 100 MB di memoria file in più, indipendentemente dalla versione di Salesforce. | **Enterprise Edition** e **Unlimited Edition** |
| `Force.com App Subscription` | Permette agli utenti di accedere a un'applicazione Force.com Light o Force.com Enterprise, nessuna delle quali è dotata di funzionalità CRM.<br><br>Un'applicazione Force.com Light dispone di un massimo di 10 oggetti personalizzati e di 10 schede personalizzate, consente l'accesso in sola lettura ad account e referenti e supporta la protezione a livello di oggetto e di campo. Un'applicazione Force.com Light non può utilizzare l'API in blocco o Streaming API.<br><br>Un'applicazione Force.com Enterprise dispone di un massimo di 10 oggetti personalizzati e di 10 schede personalizzate. Oltre alle autorizzazioni di un'applicazione Force.com Light, un'applicazione Force.com Enterprise supporta la condivisione a livello di record, può utilizzare l'API in blocco e Streaming API e dispone di accesso in lettura/scrittura ad account e referenti.<br><br>Nota: gli utenti che dispongono di questa licenza possono visualizzare i cruscotti digitali soltanto se anche l'utente in esecuzione dispone della stessa licenza.<br><br>Ogni licenza Force.com App Subscription offre ulteriori 20 MB di memoria dati per utente per la versione Enterprise Edition e 120 MB di memoria dati per utente per le versioni Unlimited e Performance Edition, oltre a 2 GB di memoria file indipendentemente dalla versione. | **Enterprise Edition**, **Unlimited Edition** e **Performance Edition** |
| `Employee Community User` | Questa è una licenza utente interna, progettata per consentire agli utenti di accedere agli oggetti e alle schede personalizzate dell'applicazione | **Enterprise Edition**, **Unlimited Edition**, |

| Tipo di licenza | Descrizione | Disponibile in |
|---|---|---|
| | Force.com Light, a Chatter (persone, gruppi, feed, file) e a una comunità dotata di un sito Site.com.<br>Gli utenti Company Community dispongono di accesso in sola lettura agli articoli di Salesforce Knowledge e di accesso limitato ai casi per creare e leggere casi personali. Gli utenti possono inoltre:<br>• Accedere a un massimo di 10 oggetti personalizzati e di 10 schede personalizzate<br>• Utilizzare contenuti, idee e risposte<br>• Utilizzare attività, operazioni, calendari ed eventi<br>• Accedere in sola lettura ad account e referenti | **Performance Edition** e **Developer Edition**. |

VEDERE ANCHE:

Panoramica sulle licenze utente

## Licenze utente Chatter

Tutte le licenze Salesforce standard consentono l'accesso gratuito a Chatter a tutti gli utenti dell'organizzazione. Inoltre, Salesforce offre licenze specifiche per Chatter: Chatter External, Chatter Free e Chatter Only (detta anche Chatter Plus).

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Licenze Chatter External e Chatter Free disponibili nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Contact Manager Edition** e **Developer Edition**

Licenze Chatter Only (noto anche come Chatter Plus) disponibili nelle versioni: **Professional Edition**, **Enterprise Edition Unlimited Edition** e **Performance Edition**

### Chatter External

Questa licenza è destinata agli utenti esterni al dominio email della società. Questi utenti esterni, detti anche clienti, possono essere invitati nei gruppi Chatter che consentono la presenza di clienti. I clienti possono accedere alle informazioni e interagire con gli utenti solo nei gruppi a cui sono stati invitati. Non possono accedere, invece, ad alcun oggetto o dato di Chatter.

### Chatter Free

La licenza Chatter Free è destinata agli utenti sprovvisti di licenze Salesforce ma che devono poter accedere a Chatter. Questi utenti possono accedere agli elementi standard di Chatter come le persone, i profili, i gruppi e i file, ma non possono accedere a oggetti o dati di Salesforce. Gli utenti Chatter Free possono anche essere moderatori di Chatter.

Gli utenti Chatter Free non vedono le schede come gli altri utenti di Salesforce. Gli utenti Chatter Free accedono ai feed, alle persone, ai gruppi e ai file mediante i link presenti nell'intestazione laterale della pagina.

Gli amministratori di Salesforce possono aggiornare una licenza Chatter Free trasformandola in licenza Salesforce standard o in licenza Chatter Only in qualsiasi momento. Non è possibile convertire una licenza Salesforce standard o una licenza Chatter Only in una licenza Chatter Free.

## Chatter Only (Chatter Plus)

La licenza Chatter Only è nota anche come licenza Chatter Plus. È destinata agli utenti che non dispongono di licenze Salesforce ma che devono poter accedere ad alcuni oggetti di Salesforce oltre che a Chatter. Gli utenti Chatter Plus possono essere moderatori di Chatter e avere accesso alle pagine standard di Chatter come le persone, i profili, i gruppi e i file. Gli utenti possono inoltre:

- Visualizzare gli account e i referenti Salesforce
- Utilizzare Salesforce CRM Content, Ideas e Risposte
- Accedere a cruscotti digitali e rapporti
- Utilizzare e approvare flussi di lavoro
- Utilizzare il calendario per creare attività e tenerne traccia
- Visualizzare e modificare fino a dieci oggetti personalizzati
- Aggiungere record ai gruppi

Per impostazione predefinita, le schede per gli oggetti standard di Salesforce sono nascoste agli utenti Chatter Plus. Rendere visibili le schede se si desidera metterle a disposizione degli utenti Chatter Plus. Per ulteriori informazioni sugli utenti Chatter Plus, vedere *Chatter Plus Frequently Asked Questions* *(disponibile solo in inglese)*.

## Panoramica sulle licenze Chatter

Questa tabella mostra l'elenco delle funzioni disponibili per le licenze Chatter External, Chatter Free e Chatter Only.

| **Funzione** | **Chatter External**<br>**(accesso limitato agli elementi e alle persone dei gruppi a cui i clienti sono invitati)** | **Chatter Free** | **Chatter Only**<br>**(noto anche come Chatter Plus)** |
|---|---|---|---|
| Client Chatter Desktop | ✓ | ✓ | ✓ |
| Uso dell'app mobile Salesforce1<br>(le app scaricabili richiedono l'autorizzazione "API abilitata" sul profilo) | ✓<br>Gli utenti delle app scaricabili non possono accedere alle visualizzazioni elenco Gruppi o Persone. | ✓ | ✓ |
| Feed | ✓ | ✓ | ✓ |
| Condivisione di file | ✓ | ✓ | ✓ |
| Gruppi | ✓ | ✓ | ✓ |
| Inviti a entrare nei gruppi | ✓<br>Solo i clienti che sono anche responsabili di gruppi possono invitare gli utenti Chatter dai gruppi a cui possono accedere o persone esterne a Chatter. | ✓ | ✓ |
| Profili | ✓ | ✓ | ✓ |

| Funzione | Chatter External (accesso limitato agli elementi e alle persone dei gruppi a cui i clienti sono invitati) | Chatter Free | Chatter Only (noto anche come Chatter Plus) |
|---|---|---|---|
| Argomenti e hashtag | ✓ | ✓ | ✓ |
| Messaggi privati | ✓ | ✓ | ✓ |
| Ricerca globale | ✓ I risultati della ricerca comprendono solo gli elementi a cui i clienti possono accedere tramite i gruppi. | ✓ | ✓ |
| Oggetti personalizzati | | | ✓ Fino a 10 oggetti personalizzati |
| Account e referenti | | | ✓ Sola lettura |
| Calendario ed eventi | | | ✓ |
| Libreria di contenuti | | | ✓ |
| Idee e risposte | | | ✓ |
| Rapporti e cruscotti digitali | | | ✓ |
| Operazioni e attività | | | ✓ |
| Uso e approvazione dei flussi di lavoro | | | ✓ |

## Licenze utente comunità

Esistono tre licenze comunità per gli utenti esterni: Customer Community, Customer Community Plus e Partner Community.

La licenza Customer Community è simile alla licenza Portale Clienti a volume elevato ed è adatta per le comunità business-to-consumer con moltissimi utenti esterni. La licenza Customer Community Plus è simile a una licenza Portale Clienti — Amministrazione aziendale ed è adatta per le comunità business-to-consumer i cui utenti necessitano di accesso illimitato per gestire l'assistenza clienti. La licenza Partner Community è simile a una licenza Partner oro ed è adatta per le comunità business-to-business come le comunità partner.

Oltre alle nuove licenze, le comunità supportano tutte le licenze interne e portale, comprese le licenze Portale Clienti, Sito Web autenticato e Portale partner esistenti. Le comunità non supportano la licenza Chatter External.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Performance Edition**, **Unlimited Edition**, **Developer Edition** ed **Enterprise Edition**

Le licenze comunità sono associate agli utenti, non a una comunità specifica. Se necessario è possibile spostare gli utenti con queste licenze da una comunità all'altra. Inoltre, le licenze inutilizzate si possono assegnare agli utenti di qualsiasi comunità dell'organizzazione.

Le licenze Customer Community, Customer Community Plus e Partner Community sono disponibili anche come licenze basate sugli accessi mensili. Questo significa che viene consumata una licenza ogni volta che un utente accede a una comunità, ma non quando un utente registrato passa da una all'altra delle sue comunità. Le licenze non utilizzate scadono alla fine del mese. Se un utente con licenza basata sugli accessi alle comunità accede alle comunità tramite Salesforce1, consuma un accesso la prima volta che accede o in caso di timeout della sessione.

Per evitare problemi di distribuzione e problemi di prestazioni nella qualità del servizio, è consigliabile che il numero di utenti nella comunità non superi i limiti elencati sotto. Se si richiedono utenti aggiuntivi oltre a questi limiti, rivolgersi al proprio responsabile account Salesforce. Il superamento dei limiti indicati può dare luogo a costi aggiuntivi e a una diminuzione delle prestazioni.

| Tipo di comunità | Numero di utenti |
|---|---|
| Partner Community o Customer Community Plus | 300,000 |
| Cliente | 7 milioni |

A ogni comunità è associato un sito Site.com che permette di aggiungere pagine personalizzate con l'immagine aziendale alla comunità. Gli utenti delle comunità dotati di autorizzazione "Crea e imposta comunità" dispongono automaticamente dell'accesso amministratore completo al sito Site.com di una comunità. Per consentire agli utenti delle comunità sprovvisti di autorizzazione di modificare il sito è necessario acquistare e assegnare una licenza funzioni Site.com Publisher o Site.com Contributor e assegnare un ruolo utente a livello di sito.

Questa tabella mostra le funzioni disponibili agli utenti con le licenze Customer Community, Customer Community Plus e Partner Community.

| | Customer Community | Customer Community Plus | Partner Community |
|---|---|---|---|
| **Oggetti standard Salesforce** | | | |
| Account | ✓ Lettura e Modifica | ✓ Lettura, Creazione, Modifica | ✓ Lettura, Creazione, Modifica |
| Asset | ✓ Lettura, Creazione, Modifica | ✓ Lettura, Creazione, Modifica | ✓ Lettura, Creazione, Modifica |
| Campagne | | | ✓ Lettura, Creazione e Modifica (richiede l'autorizzazione "Utente Marketing") [1] |
| Casi | ✓ Lettura, Creazione, Modifica [2] | ✓ Lettura, Creazione, Modifica | ✓ Lettura, Creazione, Modifica<br>Disabilitata per impostazione predefinita |
| Referenti | ✓ | ✓ | ✓ |
| Contratti | ✓ | ✓ | ✓ |

| | Customer Community | Customer Community Plus | Partner Community |
|---|---|---|---|
| Diritti | ✓ Lettura, Creazione, Modifica | ✓ Lettura, Creazione, Modifica | ✓ Lettura, Creazione, Modifica |
| Eventi e calendario | | | ✓ |
| Idee | ✓ Lettura, Creazione, Modifica | ✓ Lettura, Creazione, Modifica | ✓ Lettura, Creazione, Modifica |
| Lead | | | ✓ |
| Note e allegati | ✓ Non disponibile per gli account e i referenti [3] | ✓ Solo sull'elenco correlato Allegati su casi [4] | ✓ |
| Opportunità | | | ✓ |
| Ordini [5] | ✓ | ✓ | ✓ |
| Listini prezzi | ✓ Sola lettura | ✓ Sola lettura | ✓ Sola lettura |
| Prodotti | ✓ Sola lettura | ✓ Sola lettura | ✓ Sola lettura |
| Preventivi | | | ✓ |
| Rapporti e cruscotti digitali | | ✓ Sola lettura (per impostazione predefinita) Creazione e Modifica (richiede autorizzazioni utente) [6] | ✓ Sola lettura (per impostazione predefinita) Creazione e Modifica (richiede autorizzazioni utente) [6] |
| Contratti di servizio | | ✓ Lettura, Creazione, Modifica | ✓ Lettura, Creazione, Modifica |
| Operazioni | ✓ Sola lettura | ✓ Lettura, Creazione, Modifica | ✓ Lettura, Creazione, Modifica |
| **Funzioni, capacità e oggetti personalizzati di Salesforce** | | | |
| Memoria aggiuntiva | | 2 MB per membro (licenza basata sui membri) 1 MB per membro (licenza basata sugli accessi) | 5 MB per membro (licenza basata sui membri) 1 MB per membro (licenza basata sugli accessi) |
| Chatter (persone, gruppi, feed, file, messaggi privati) | ✓ | ✓ | ✓ |

| | Customer Community | Customer Community Plus | Partner Community |
|---|---|---|---|
| Nota: Salesforce Files Sync non è disponibile nelle Comunità. | | | |
| Risposte Chatter | ✓ | ✓ | ✓ |
| Content (con licenza funzioni Salesforce CRM Content) | | ✓ Visualizza e carica | ✓ Visualizza e carica |
| Content (senza licenza funzioni Salesforce CRM Content) | | ✓ Solo visualizzazione | ✓ Solo visualizzazione |
| Oggetti personalizzati | ✓ 10 oggetti personalizzati per licenza (gli oggetti personalizzati nei pacchetti gestiti non sono conteggiati in questo limite) | ✓ 10 oggetti personalizzati per licenza (gli oggetti personalizzati nei pacchetti gestiti non sono conteggiati in questo limite) | ✓ 10 oggetti personalizzati per licenza (gli oggetti personalizzati nei pacchetti gestiti non sono conteggiati in questo limite) |
| Amministrazione delegata | | ✓ | ✓ |
| Knowledge | ✓ Sola lettura | ✓ Sola lettura | ✓ Sola lettura |
| Ruoli e condivisione | | ✓ | ✓ |
| App mobile Salesforce1 | ✓ | ✓ | ✓ |
| Invia email | | | ✓ |
| Approvazioni flusso di lavoro | | ✓ | ✓ |

Nota:

- [1] Per la licenza Partner Community, per leggere, creare e modificare le campagne nell'interfaccia utente, l'utente partner deve disporre anche dell'autorizzazione "Utente Marketing". Con queste autorizzazioni, un utente partner può: cercare e aggiungere i propri referenti o lead come membri della campagna, accedere ai rapporti sulle campagne ed eseguire l'invio di email globale o l'assegnazione globale di referenti e lead a una campagna.
- [2] Per la licenza Customer Community, non è possibile creare i casi per conto di qualcun altro.
- [3] Per la licenza Customer Community, l'elenco correlato Note e allegati non è disponibile per Account e Referenti.
- [4] Per la licenza Customer Community Plus, gli allegati sono disponibili solo tramite l'elenco correlato Allegati sui casi. Le note non sono supportate.
- [5] Quando sono abilitati gli ordini, i profili standard includono automaticamente tutte le autorizzazioni relative agli oggetti per gli ordini, oltre all'accesso in lettura per prodotti e listini prezzi. Se gli utenti esterni sono assegnati a un profilo standard per cui le autorizzazioni relative agli oggetti non sono adeguate, si può pensare di creare dei profili personalizzati che non includono queste autorizzazioni per gli oggetti.

- [6] Per consentire alle licenze Customer Community Plus e Partner Community di creare e modificare i rapporti, l'utente deve disporre anche delle autorizzazioni "Crea e personalizza rapporti", "Generatore di rapporti" e "Modifica rapporti personali". Per ulteriori informazioni, vedere Configurazione della gestione dei rapporti per gli utenti esterni: creazione e modifica di rapporti.

VEDERE ANCHE:

Panoramica sulle licenze utente

Licenze utente Sito Web autenticato

Licenze utente Portale partner

Licenze utente del Portale Clienti

## Licenze utente Database.com

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nella versione: **Database.com Edition**

| Licenza utente | Descrizione | Numero predefinito di licenze disponibili |
|---|---|---|
| Amministratore di Database.com | Creata per gli utenti che devono amministrare Database.com o modificare gli schemi di Database.com o altri metadati utilizzando gli strumenti "point-and-click" nella console di Database.com. | Database.com Edition: 3 |
| Utente di Database.com | Creata per gli utenti che necessitano dell'accesso Database.com ai dati memorizzati in Database.com. | Database.com Edition: 3<br>Enterprise Edition, Unlimited Edition e Database.com Edition: 0<br>Contattare Database.com per ottenere le licenze utente Database.com |
| Utente Database.com Light | Destinata agli utenti che necessitano soltanto dell'accesso Database.com ai dati, che devono appartenere ai gruppi Database.com (ma non ad altri gruppi) e non devono appartenere a ruoli o aree di attesa. L'accesso ai dati è determinato dalle impostazioni di condivisione predefinite dell'organizzazione. | Database.com Edition: 0<br>Enterprise Edition, Unlimited Edition e Database.com Edition: 0 |

| Licenza utente | Descrizione | Numero predefinito di licenze disponibili |
| --- | --- | --- |
| | | Contattare Database.com per ottenere le licenze utente Database.com Light |

VEDERE ANCHE:

Panoramica sulle licenze utente

## Licenze utente per il Portale Service Cloud

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Gli utenti del Portale Service Cloud dispongono di licenza Portale Clienti a volume elevato. Tale licenza fornisce ai referenti un numero illimitato di accessi al Portale Service Cloud per accedere alle informazioni dell'assistenza clienti. Gli utenti con questa licenza possono accedere ad account, asset, casi, referenti, oggetti personalizzati, documenti, idee e domande, in base alle impostazioni delle rispettive autorizzazioni.

La licenza Overage High Volume Customer Portal corrisponde alla licenza Portale clienti a volume elevato con la differenza che gli utenti non dispongono di un numero illimitato di accessi. Per ulteriori informazioni sul numero di licenze Portale Clienti che è possibile attivare, rivolgersi a Salesforce.

Nella tabella che segue sono riportate le autorizzazioni che possono essere assegnate agli utenti del portale Service Cloud.

| | Crea | Lettura | Aggiorna | Elimina |
| --- | --- | --- | --- | --- |
| **Account** | | ✓ | ✓ | |
| **Asset** | ✓ | ✓ | ✓ | |
| **Casi** | ✓ | ✓ | ✓ | |
| **Referenti** | ✓ | ✓ | ✓ | |
| **Oggetti personalizzati** | ✓ | ✓ | ✓ | ✓ |
| **Documenti** | | ✓ | | |
| **Idee** | ✓ | ✓ | | |
| **Knowledge** | | ✓ | | |
| **Listini prezzi** | | ✓ | | |
| **Prodotti** | | ✓ | | |
| **Domande e risposte** | ✓ | ✓ | | |

| | Crea | Lettura | Aggiorna | Elimina |
|---|---|---|---|---|
| **Soluzioni** | | ✓ | | |

VEDERE ANCHE:

Panoramica sulle licenze utente

## Licenze utente Siti e Site.com

Gli utenti dei Siti e Site.com possono avere licenze Utente Guest o utente Site.com Only.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

I requisiti relativi alla versione (Edition) variano in base al tipo di licenza utente.

`Utente Guest`

Ideata appositamente per gli utenti pubblici che accedono ai siti Site.com o Force.com. Se sono abilitate le comunità, questi utenti possono accedere anche alle pagine pubbliche delle comunità. I visitatori dei siti hanno accesso a tutte le informazioni rese disponibili in un sito pubblico attivo. È possibile sviluppare un sito per la propria organizzazione per ogni licenza Utente Guest.

Per Site.com, le versioni **Developer Edition**, **Enterprise Edition**, **Unlimited Edition** e **Performance Edition** dispongono tutte di un numero illimitato di licenze Utente Guest.

Per i siti Force.com, le versioni **Enterprise Edition**, **Unlimited Edition** e **Performance Edition** sono fornite con 25 licenze Utente Guest ciascuna. La versione **Developer Edition** dispone di una sola licenza Utente Guest.

Nota:

- Non è possibile acquistare licenze Utente Guest aggiuntive per i siti Force.com.
- La licenza Sito Web autenticato per utenti del portale a volume elevato è stata creata appositamente per l'utilizzo con i siti Force.com. Poiché è progettata per i volumi elevati, è un'opzione conveniente per l'utilizzo con i siti Force.com.

`Site.com Only`

Ideata per gli utenti delle versioni **Performance Edition**, **Unlimited Edition** ed **Enterprise Edition** che devono poter accedere a Site.com ma non alle funzionalità CRM standard. Gli utenti Site.com Only dispongono degli stessi diritti degli utenti Force.com - One App, più l'accesso all'applicazione Content. Non possono invece accedere agli oggetti Account e Referenti. Gli utenti possono accedere a un numero illimitato di schede personalizzate ma possono utilizzare una sola applicazione personalizzata composta da un massimo di 20 oggetti personalizzati.

Ogni utente Site.com Only necessita inoltre di una licenza funzioni Site.com Contributor o Site.com Publisher per accedere a Site.com.

VEDERE ANCHE:

Panoramica sulle licenze utente

## Licenze utente Sito Web autenticato

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Gli utenti del Portale piattaforma dispongono di licenza Sito Web autenticato, che è stata creata appositamente per l'uso con Force.com Sites. Fornisce agli utenti denominati dei siti un numero illimitato di accessi al Portale Piattaforma per accedere alle informazioni di assistenza clienti.

La licenza Overage Authenticated Website corrisponde alla licenza Sito Web autenticato, tranne per il fatto che gli utenti non dispongono di un numero illimitato di accessi.

Nota: Quando sono abilitati gli ordini, i profili standard includono automaticamente tutte le autorizzazioni relative agli oggetti per gli ordini, oltre all'accesso in lettura per prodotti e listini prezzi. Se gli utenti esterni sono assegnati a un profilo standard per cui le autorizzazioni relative agli oggetti non sono adeguate, si può pensare di creare dei profili personalizzati che non includono queste autorizzazioni per gli oggetti.

Nella tabella che segue sono riportate le autorizzazioni che possono essere concesse agli utenti Sito Web autenticato.

| | Crea | Lettura | Aggiorna | Elimina |
|---|---|---|---|---|
| **Contratti** | ✓ | ✓ | ✓ | ✓ |
| **Documenti** | | ✓ | | |
| **Idee** | ✓ | ✓ | | |
| **Knowledge** | | ✓ | | |
| **Ordini** | ✓ | ✓ | ✓ | ✓ |
| **Listini prezzi** | | ✓ | | |
| **Prodotti** | | ✓ | | |
| **Oggetti personalizzati** | ✓ | ✓ | ✓ | ✓ |

VEDERE ANCHE:

Panoramica sulle licenze utente

## Licenze utente del Portale Clienti

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Gli utenti di un sito Portale Clienti dispongono di licenza Responsabile Portale Clienti standard.

Nota: a partire dal rilascio Summer '13, queste licenze sono disponibili solo per le organizzazioni che dispongono già di un Portale Clienti. Se non si dispone di un Portale Clienti ma si desidera condividere facilmente le informazioni con i propri clienti, vedere Licenze utente comunità a pagina 162.

Consente ai referenti di accedere al Portale Clienti per gestire l'assistenza ai clienti. Gli utenti con una licenza Responsabile Portale Clienti (standard) possono essere associati al profilo Utente Portale Clienti o a un profilo clonato e personalizzato dal profilo Utente Portale Clienti. Questo profilo standard consente agli utenti di visualizzare e modificare i dati di cui sono direttamente i titolari o i dati di proprietà o condivisi con utenti posti a un livello inferiore nella gerarchia dei ruoli del Portale Clienti. Questi utenti possono anche visualizzare e modificare i casi in cui sono elencati nel campo `Nome referente`.

Gli utenti con la licenza Responsabile Portale Clienti (standard) possono:

- Visualizzare referenti, listini prezzi e prodotti.
- Visualizzare e modificare account e casi.
- Creare e modificare asset.
- Creare, visualizzare, modificare ed eliminare oggetti personalizzati.
- Accedere agli oggetti personalizzati in base alle rispettive autorizzazioni.
- Ricevere l'autorizzazione "Super utente portale".
- Accedere a Salesforce CRM Content se dispongono di una licenza funzioni Salesforce CRM Content o delle opportune autorizzazioni.

La licenza Overage Customer Portal Manager (standard) corrisponde alla licenza Responsabile Portale Clienti (personalizzata), tranne per il fatto che gli utenti sono limitati a un accesso al mese.

Nota: Quando sono abilitati gli ordini, i profili standard includono automaticamente tutte le autorizzazioni relative agli oggetti per gli ordini, oltre all'accesso in lettura per prodotti e listini prezzi. Se gli utenti esterni sono assegnati a un profilo standard per cui le autorizzazioni relative agli oggetti non sono adeguate, si può pensare di creare dei profili personalizzati che non includono queste autorizzazioni per gli oggetti.

Nella tabella che segue sono riportate le autorizzazioni che possono essere concesse agli utenti del Portale Clienti.

| | Crea | Lettura | Aggiorna | Elimina |
|---|---|---|---|---|
| **Account** | | ✓ | ✓ | |
| **Asset** | ✓ | ✓ | ✓ | |
| **Casi** | ✓ | ✓ | ✓ | |
| **Referenti** | | ✓ | | |
| **Contratti** | ✓ | ✓ | ✓ | ✓ |
| **Oggetti personalizzati** | ✓ | ✓ | ✓ | ✓ |
| **Documenti** | | ✓ | | |
| **Idee** | ✓ | ✓ | ✓ | |
| **Knowledge** | | ✓ | | |
| **Ordini** | ✓ | ✓ | ✓ | ✓ |
| **Listini prezzi** | | ✓ | | |
| **Prodotti** | | ✓ | | |
| **Soluzioni** | | ✓ | | |
| **Domande e risposte** | ✓ | ✓ | | |

VEDERE ANCHE:

Panoramica sulle licenze utente

## Licenze utente del Portale Clienti — Amministrazione aziendale

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Gli utenti del Portale Clienti — Amministrazione aziendale dispongono della licenza Responsabile Portale Clienti personalizzata. Questa licenza fornisce ai referenti un numero illimitato di accessi al Portale Clienti Salesforce per gestire l'assistenza clienti.

Nota: a partire dal rilascio Summer '13, queste licenze sono disponibili solo per le organizzazioni che dispongono già di un Portale Clienti. Se non si dispone di un Portale Clienti ma si desidera condividere facilmente le informazioni con i propri clienti, vedere Licenze utente comunità a pagina 162.

Gli utenti con una licenza Responsabile Portale Clienti (personalizzata) possono essere associati al profilo Utente Portale Clienti o a un profilo clonato e personalizzato dal profilo Utente Portale Clienti, il che consente loro di visualizzare e modificare i dati di cui sono direttamente titolari e di visualizzare, creare e modificare i casi in cui sono elencati nel campo `Nome referente`.

Gli utenti con questa licenza possono:

- Creare, leggere o aggiornare account, asset e casi.
- Visualizzare i referenti.
- Visualizzare gli oggetti personalizzati ed eseguire rapporti in base alle rispettive autorizzazioni.
- Ricevere le autorizzazioni "Super utente portale" e "Amministratore utente esterno delegato".
- Accedere a Salesforce CRM Content se dispongono di una licenza funzioni Salesforce CRM Content o delle opportune autorizzazioni.

La licenza Overage Customer Portal Manager (personalizzata) corrisponde alla licenza Responsabile Portale Clienti (personalizzata), tranne per il fatto che gli utenti non dispongono di un numero illimitato di accessi. Per ulteriori informazioni sul numero di licenze Portale Clienti che è possibile attivare, rivolgersi a Salesforce.

Nota: Quando sono abilitati gli ordini, i profili standard includono automaticamente tutte le autorizzazioni relative agli oggetti per gli ordini, oltre all'accesso in lettura per prodotti e listini prezzi. Se gli utenti esterni sono assegnati a un profilo standard per cui le autorizzazioni relative agli oggetti non sono adeguate, si può pensare di creare dei profili personalizzati che non includono queste autorizzazioni per gli oggetti.

Nella tabella che segue sono riportate le autorizzazioni che possono essere concesse agli utenti del Portale Clienti — Amministrazione aziendale.

| | Crea | Lettura | Aggiorna | Elimina |
|---|---|---|---|---|
| **Account** | ✓ | ✓ | ✓ | |
| **Asset** | ✓ | ✓ | ✓ | |
| **Casi** | ✓ | ✓ | ✓ | |
| **Referenti** | ✓ | ✓ | ✓ | |
| **Contratti** | ✓ | ✓ | ✓ | ✓ |
| **Oggetti personalizzati** | ✓ | ✓ | ✓ | ✓ |
| **Documenti** | | ✓ | | |
| **Idee** | ✓ | ✓ | ✓ | |
| **Knowledge** | | ✓ | | |
| **Ordini** | ✓ | ✓ | ✓ | ✓ |

| | Crea | Lettura | Aggiorna | Elimina |
|---|---|---|---|---|
| **Listini prezzi** | | ✓ | | |
| **Prodotti** | | ✓ | | |
| **Soluzioni** | | ✓ | | |
| **Domande e risposte** | ✓ | ✓ | | |

VEDERE ANCHE:

Panoramica sulle licenze utente

## Licenze utente Portale partner

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Gli utenti del Portale partner dispongono della licenza utente Partner oro. Possono accedere a Salesforce solo tramite il Portale partner.

Nota:

- a partire dal rilascio Summer '13, questa licenza non sarà più disponibile per le organizzazioni che non utilizzano già il Portale partner. Se non si dispone di un Portale partner ma si desidera condividere facilmente le informazioni con i propri partner, vedere Licenze utente comunità a pagina 162.
- Quando sono abilitati gli ordini, i profili standard includono automaticamente tutte le autorizzazioni relative agli oggetti per gli ordini, oltre all'accesso in lettura per prodotti e listini prezzi. Se gli utenti esterni sono assegnati a un profilo standard per cui le autorizzazioni relative agli oggetti non sono adeguate, si può pensare di creare dei profili personalizzati che non includono queste autorizzazioni per gli oggetti.

Nella tabella che segue sono riportate le autorizzazioni che possono essere concesse agli utenti del Portale partner.

| | Crea | Lettura | Aggiorna | Elimina |
|---|---|---|---|---|
| **Account** | ✓ | ✓ | ✓ | |
| **Approvazioni** | | ✓ | | |
| **Asset** | ✓ | ✓ | ✓ | |
| **Campagne**[1] | ✓ | ✓ | ✓ | |
| **Casi** | ✓ | ✓ | ✓ | |
| **Referenti** | ✓ | ✓ | ✓ | |
| **Contratti** | ✓ | ✓ | ✓ | ✓ |
| **Oggetti personalizzati** | ✓ | ✓ | ✓ | ✓ |
| **Documenti** | | ✓ | | |
| **Idee** | ✓ | ✓ | ✓ | |
| **Knowledge** | | ✓ | | |

| | Crea | Lettura | Aggiorna | Elimina |
|---|---|---|---|---|
| **Lead** | ✓ | ✓ | ✓ | |
| **Opportunità** | ✓ | ✓ | ✓ | |
| **Ordini** | ✓ | ✓ | ✓ | ✓ |
| **Listini prezzi** | | ✓ | | |
| **Prodotti** | | ✓ | | |
| **Soluzioni** | | ✓ | | |
| **Domande e risposte** | ✓ | ✓ | | |

[1] L'utente di un portale partner può creare e modificare le campagne in una comunità ma non in un portale precedente. Per consentire alla licenza Partner Community di leggere, creare e modificare le campagne nell'interfaccia utente, l'utente partner deve disporre anche dell'autorizzazione "Utente Marketing". Con queste autorizzazioni, un utente partner può: cercare e aggiungere i propri referenti o lead come membri della campagna, accedere ai rapporti sulle campagne ed eseguire l'invio di email globale o l'assegnazione globale di referenti e lead a una campagna.

VEDERE ANCHE:

Panoramica sulle licenze utente

## Licenze insieme di autorizzazioni

Un insieme di autorizzazioni è un metodo comodo per assegnare agli utenti impostazioni e autorizzazioni specifiche per l'uso di svariati strumenti e funzioni.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

La disponibilità di ogni singola licenza insieme di autorizzazioni dipende dai requisiti della versione (Edition) per gli insiemi di autorizzazioni e dalla relativa funzione.

IN QUESTA SEZIONE:

Cosa sono le licenze insieme di autorizzazioni?

Le licenze insieme di autorizzazioni consentono agli utenti di accedere via via a nuove funzioni che non sono incluse nelle loro licenze utente. Agli utenti può essere assegnato un numero qualsiasi di licenze insieme di autorizzazioni.

Licenze insieme di autorizzazioni disponibili

Per ogni licenza insieme di autorizzazione acquistabile, vedere quali autorizzazioni consente di assegnare agli utenti.

Visualizzazione delle licenze insieme di autorizzazioni dell'organizzazione

Visualizzare le licenze insieme di autorizzazioni acquistate dall'organizzazione per vedere quali sono disponibili per l'assegnazione agli utenti.

Assegnazione di una licenza insieme di autorizzazioni a un utente

Per alcune autorizzazioni è necessario assegnare all'utente una licenza insieme di autorizzazioni e quindi aggiungere le autorizzazioni agli insiemi di autorizzazioni.

Rimozione della licenza insieme di autorizzazioni di un utente

Innanzitutto, rimuovere o modificare gli insiemi di autorizzazioni assegnati che richiedono la licenza, e quindi eliminare la licenza insieme di autorizzazione assegnata.

VEDERE ANCHE:

Come trovare informazioni sulla società

## Cosa sono le licenze insieme di autorizzazioni?

Le licenze insieme di autorizzazioni consentono agli utenti di accedere via via a nuove funzioni che non sono incluse nelle loro licenze utente. Agli utenti può essere assegnato un numero qualsiasi di licenze insieme di autorizzazioni.

In quanto licenze aggiuntive, le licenze insieme di autorizzazioni non limitano le funzionalità. Le licenze insieme di autorizzazioni consentono di assegnare agli utenti un numero maggiore di autorizzazioni rispetto a quelle supportate dalle rispettive licenze utente.

Dopo avere assegnato una licenza insieme di autorizzazioni a un utente, assegnargli le autorizzazioni appropriate tramite un insieme di autorizzazioni (e non un profilo).

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

La disponibilità di ogni singola licenza insieme di autorizzazioni dipende dai requisiti della versione (Edition) per gli insiemi di autorizzazioni e dalla relativa funzione.

Esempio:

- Per poter assegnare a un utente un insieme di autorizzazioni con l'autorizzazione "Utilizza Identity Connect", è necessario prima assegnargli una licenza insieme di autorizzazioni Identity Connect.
- Per poter assegnare a un utente con licenza utente Force.com un insieme di autorizzazioni con l'autorizzazione "Lettura" o "Modifica" per gli ordini, è necessario prima assegnargli una licenza insieme di autorizzazioni piattaforma Ordini. Queste autorizzazioni si possono assegnare a un utente con licenza utente Salesforce senza una licenza insieme di autorizzazioni, in quanto questa è già abilitata nella licenza utente.

VEDERE ANCHE:

Licenze insieme di autorizzazioni

## Licenze insieme di autorizzazioni disponibili

Per ogni licenza insieme di autorizzazione acquistabile, vedere quali autorizzazioni consente di assegnare agli utenti.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

La disponibilità di ogni singola licenza insieme di autorizzazioni dipende dai requisiti della versione (Edition) per gli insiemi di autorizzazioni e dalla relativa funzione.

| Licenza insieme di autorizzazioni | Autorizzazioni utente incluse | Autorizzazioni oggetto incluse |
|---|---|---|
| Employee Community User per Force.com | "Consenti Visualizza Knowledge" | "Crea" e "Lettura" per i casi |
| Files Connect per fonti di dati esterne in loco | “Files Connect in loco" | |
| Identity Connect | "Utilizza Identity Connect" | |

| Licenza insieme di autorizzazioni | Autorizzazioni utente incluse | Autorizzazioni oggetto incluse |
|---|---|---|
| Piattaforma Ordini | • "Attiva contratti"<br>• "Elimina contratti attivati"<br>• "Attiva ordini"<br>• "Modifica ordini attivati"<br>• "Crea ordini di riduzione" | "Crea", "Lettura", "Modifica" ed "Elimina" per:<br>• Contratti<br>• Listini prezzi<br>• Prodotti<br>• Ordini |
| Utente Console Sales | "Console Sales" | |

VEDERE ANCHE:

Assegnazione di una licenza insieme di autorizzazioni a un utente

Autorizzazioni utente

Assegnare insiemi di autorizzazioni a un unico utente

Licenze insieme di autorizzazioni

## Visualizzazione delle licenze insieme di autorizzazioni dell'organizzazione

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le licenze insieme di autorizzazioni:

- "Visualizza impostazione e configurazione"

Visualizzare le licenze insieme di autorizzazioni acquistate dall'organizzazione per vedere quali sono disponibili per l'assegnazione agli utenti.

1. Da Imposta, immettere `Informazioni sulla società` nella casella `Ricerca veloce`, quindi selezionare **Informazioni sulla società**.
2. Visualizzare l'elenco correlato Licenze insieme di autorizzazioni.

Per informazioni sull'acquisto delle licenze insieme di autorizzazioni, contattare Salesforce.

VEDERE ANCHE:

Licenze insieme di autorizzazioni

Licenze insieme di autorizzazioni disponibili

Assegnazione di una licenza insieme di autorizzazioni a un utente

## Assegnazione di una licenza insieme di autorizzazioni a un utente

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per assegnare una licenza insieme di autorizzazioni:

- "Gestisci utenti"

Per alcune autorizzazioni è necessario assegnare all'utente una licenza insieme di autorizzazioni e quindi aggiungere le autorizzazioni agli insiemi di autorizzazioni.

1. Da Imposta, immettere `Utenti` nella casella `Ricerca veloce`, quindi selezionare **Utenti**.
2. Fare clic sul nome dell'utente a cui si desidera assegnare la licenza insieme di autorizzazioni.
3. Nell'elenco correlato Assegnazioni licenze insieme di autorizzazioni, fare clic su **Modifica assegnazioni**.
4. Selezionare la licenza insieme di autorizzazioni da assegnare all'utente e fare clic su **Salva**.

Dopo avere assegnato a un utente una licenza insieme di autorizzazioni, aggiungere la relativa autorizzazione a un insieme di autorizzazioni e assegnarlo all'utente.

VEDERE ANCHE:

Licenze insieme di autorizzazioni
Rimozione della licenza insieme di autorizzazioni di un utente
Insiemi di autorizzazioni
Assegnare insiemi di autorizzazioni a un unico utente

## Rimozione della licenza insieme di autorizzazioni di un utente

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per rimuovere una licenza insieme di autorizzazioni:

- "Gestisci utenti"

Innanzitutto, rimuovere o modificare gli insiemi di autorizzazioni assegnati che richiedono la licenza, e quindi eliminare la licenza insieme di autorizzazione assegnata.

1. Individuare l'autorizzazione che richiede la licenza insieme di autorizzazioni che si desidera rimuovere.
2. Controllare che l'autorizzazione non sia assegnata all'utente tramite un insieme di autorizzazioni, in uno dei modi seguenti.
   - Rimuovere l'autorizzazione dagli insiemi di autorizzazioni assegnati all'utente
   - Rimuovere l'insieme di autorizzazioni dagli insiemi di autorizzazioni assegnati all'utente
3. Da Imposta, immettere `Utenti` nella casella `Ricerca veloce`, quindi selezionare **Utenti**.
4. Fare clic sul nome dell'utente di cui si desidera rimuovere la licenza insieme di autorizzazioni.
5. Nell'elenco correlato Assegnazioni licenze insieme di autorizzazioni, fare clic su **Modifica assegnazioni**.
6. Deselezionare la licenza insieme di autorizzazioni appropriata.
7. Fare clic su **Salva**.

VEDERE ANCHE:

Licenze insieme di autorizzazioni
Visualizzazione delle licenze insieme di autorizzazioni dell'organizzazione
Assegnazione di una licenza insieme di autorizzazioni a un utente

# Panoramica sulle licenze funzioni

Una licenza funzioni consente a un utente di accedere a una funzione aggiuntiva non inclusa nella sua licenza utente, ad esempio Marketing o Work.com. È possibile assegnare agli utenti un numero illimitato di licenze funzioni.

- Visualizzare le licenze funzioni abilitate per la propria organizzazione
- Consentire agli utenti di usare una funzione
- Vedere tutte le licenze funzioni attualmente disponibili in Salesforce

A seconda delle funzioni abilitate per la propria organizzazione, può essere possibile assegnare agli utenti più tipi di licenze funzioni.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

I requisiti relativi alla versione (Edition) variano per ogni licenza funzioni.

VEDERE ANCHE:

Visualizzazione e gestione degli utenti

Acquisto di più licenze per gli utenti

Come trovare informazioni sulla società

## Visualizzazione delle licenze funzioni dell'organizzazione

Visualizzare le licenze funzioni acquistate dalla propria azienda per vedere quali sono disponibili per l'assegnazione agli utenti.

1. Da Imposta, immettere *`Informazioni sulla società`* nella casella `Ricerca veloce`, quindi selezionare **Informazioni sulla società**.
2. Consultare l'elenco correlato Licenze funzioni.

Per informazioni sull'acquisto di licenze funzioni, contattare Salesforce.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le licenze funzioni:

- "Visualizza impostazione e configurazione"

VEDERE ANCHE:

Panoramica sulle licenze funzioni

Licenze funzioni disponibili

Abilitazione di una licenza funzioni per un utente

Visualizzazione e gestione degli utenti

Acquisto di più licenze per gli utenti

## Abilitazione di una licenza funzioni per un utente

È possibile abilitare una funzione per un utente dell'organizzazione quando crea o si modifica l'utente.

1. In Imposta, immettere *Utenti* nella casella `Ricerca veloce`, quindi selezionare **Utenti**.
2. Nella visualizzazione elenco degli utenti, fare clic sul nome di un utente.
3. Nella pagina Dettaglio utente, selezionare la casella di controllo accanto alla licenza funzioni da abilitare per quell'utente.

   Per un singolo utente è possibile abilitare più licenze funzioni.

4. Fare clic su **Salva**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per abilitare le licenze funzioni:

- "Gestisci utenti interni"

VEDERE ANCHE:

Modifica degli utenti
Aggiunta di un singolo utente
Panoramica sulle licenze funzioni
Licenze funzioni disponibili
Visualizzazione delle licenze funzioni dell'organizzazione

## Licenze funzioni disponibili

Assegnare agli utenti una o più di queste licenze funzioni supplementari per consentire l'accesso a funzioni non incluse nelle rispettive licenze utente.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

| Licenza funzioni | Consente all'utente di |
| --- | --- |
| `Utente Risposte Chatter` | Accedere a Risposte Chatter. Questa licenza funzioni viene assegnata automaticamente agli utenti del portale a volume elevato che si autoregistrano per Risposte Chatter. |
| `Utente Force.com Flow` | Eseguire i flussi. |
| `Utente Knowledge` | Accedere a Salesforce Knowledge. |
| `Utente Live Agent` | Accedere a Live Agent. |
| `Utente Marketing` | Creare, modificare ed eliminare campagne, configurare le impostazioni avanzate delle campagne, importare lead e aggiornare la cronologia delle campagne tramite l'importazione guidata dei membri. |
| `Utente mobile` | Accedere a Salesforce Classic mobile. la casella di controllo `Utente mobile` non è valida per la versione gratuita di Salesforce Classic mobile perché gli utenti di questa app possono accedere a Salesforce dal loro dispositivo senza una licenza mobile. |

| Licenza funzioni | Consente all'utente di |
|---|---|
| `Utente Offline` | Accedere a Connect Offline. |
| `Utente Salesforce CRM Content` | Accedere a Salesforce CRM Content. |
| `Utente Service Cloud` | Accedere alla Salesforce Console for Service.<br>Nota: l'accesso alla Salesforce Console for Sales richiede la licenza insieme di autorizzazioni `Utente Console Sales`. |
| `Utente Site.com Contributor` | Modificare il contenuto dei siti in Site.com Studio. |
| `Utente Site.com Publisher` | Creare siti Web e definirne gli stili, controllare il layout e il funzionamento delle pagine e degli elementi di pagina, aggiungere e modificare i contenuti in Site.com Studio. |
| `Utente Work.com` | Accedere agli oggetti e alle autorizzazioni Work.com. |

VEDERE ANCHE:

Visualizzazione delle licenze funzioni dell'organizzazione

Abilitazione di una licenza funzioni per un utente

Visualizzazione e gestione degli utenti

Panoramica sulle licenze funzioni

## Panoramica sui diritti basati sull'utilizzo

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

Un diritto basato sull'utilizzo è una risorsa limitata che l'organizzazione può utilizzare in un periodo di tempo prestabilito, ad esempio il numero di accessi mensili consentiti a una comunità partner o il limite di record per gli utenti Data.com List.

Alcuni diritti sono costanti. Essi danno all'organizzazione la possibilità di utilizzare una certa risorsa con un limite fisso, e la quantità consentita non cambia a meno che non sia modificato il contratto. Ad esempio, se l'organizzazione acquista abbonamenti mensili per l'accesso a una comunità partner per 50 membri, è possibile assegnare a un massimo di 50 persone la possibilità di accedere alla comunità ogni volta che lo desiderano.

Altri diritti non sono costanti e funzionano come crediti. L'organizzazione può utilizzare tutta la quantità consentita di un diritto nel periodo indicato dalla frequenza della risorsa. Se il diritto ha frequenza "Una volta", l'organizzazione dovrà acquistare altra risorsa per reintegrare la sua riserva. Se il diritto ha frequenza "Mensile", l'inizio e la fine del mese sono determinati dal contratto e non dal mese di calendario.

Ad esempio:

- La società A acquista 50 accessi mensili per una comunità partner. Il 15 gennaio dispone di una dotazione di 50 accessi. Ogni volta che qualcuno accede, viene consumato un accesso. Il 15 febbraio, indipendentemente dal numero di accessi utilizzati nel mese precedente, la dotazione viene aggiornata e altri 50 accessi sono disponibili fino al 14 marzo.
- La società B acquista 2.000 record per gli utenti Data.com List, con data finale 15 maggio. Fino a quella data, gli utenti List dell'organizzazione potranno aggiungere o esportare fino a 2.000 record. Se l'organizzazione raggiunge questo limite prima del 15 maggio, gli utenti Data.com List non potranno aggiungere o esportare altri record. Per sbloccare gli utenti, la società B può acquistare una riserva aggiuntiva di quella risorsa.

Nota: se l'organizzazione ha più contratti che interessano la medesima `Risorsa` e l'`ID risorsa è (tenant)`, sarà comunque visualizzata una sola riga per quel diritto, ma i dati di quella riga saranno relativi a tutti i contratti. In questo caso, la `Data iniziale` è la prima data iniziale fra quelle di tutti i contratti, e la `Data finale` è l'ultima data finale fra quelle di tutti i contratti.

Come le licenze funzioni, i diritti basati sull'utilizzo non pongono limiti alle operazioni eseguibili in Salesforce, ma aumentano le funzionalità disponibili. Se l'utilizzo supera il limite stabilito, Salesforce si metterà in contatto per esaminare un'eventuale estensione del contratto.

IN QUESTA SEZIONE:

Visualizzazione dei diritti basati sull'utilizzo dell'organizzazione
Come visualizzare i diritti basati sull'utilizzo della società per sapere a quali risorse ha diritto la propria organizzazione.

Campi diritti basati sull'utilizzo

VEDERE ANCHE:

Come trovare informazioni sulla società

Visualizzazione e gestione degli utenti

## Visualizzazione dei diritti basati sull'utilizzo dell'organizzazione

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare i diritti basati sull'utilizzo:

- "Visualizza impostazione e configurazione"

Come visualizzare i diritti basati sull'utilizzo della società per sapere a quali risorse ha diritto la propria organizzazione.

1. Da Imposta, immettere *`Informazioni sulla società`* nella casella `Ricerca veloce`, quindi selezionare **Informazioni sulla società**.
2. In fondo alla pagina Informazioni sulla società, visualizzare l'elenco correlato Diritti basati sull'utilizzo.

VEDERE ANCHE:

Panoramica sui diritti basati sull'utilizzo

Campi diritti basati sull'utilizzo

## Campi diritti basati sull'utilizzo

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

Nell'elenco correlato Diritti basati sull'utilizzo compaiono le seguenti informazioni. Questi campi non sono modificabili e sono visibili solo se l'organizzazione ha diritto all'utilizzo di una risorsa.

| Nome colonna | Descrizione |
| --- | --- |
| `Risorsa` | La risorsa che la società può utilizzare. |
| `ID risorsa` | Identificatore univoco di questa voce. |

| Nome colonna | Descrizione |
|---|---|
| `Data iniziale` | Il giorno di decorrenza del contratto.<br>Nota: Se più contratti interessano quella risorsa, il campo riporta la prima data iniziale fra quelle dei vari contratti. |
| `Data finale` | Il giorno di scadenza del contratto.<br>Nota: Se più contratti interessano quella risorsa, il campo riporta l'ultima data finale fra quelle dei vari contratti. |
| `Frequenza` | Se Mensile, `Quantità consentita` viene azzerato alla fine di ogni mese.<br>Se Una volta, la `Quantità consentita` è disponibile fino alla `Data finale`. |
| `Quantità consentita` | Quantità di una risorsa che l'organizzazione può utilizzare. Se la `Frequenza` è Mensile, il mese inizia alla `Data iniziale`. |
| `Ammontare utilizzato` | Quantità di una risorsa che l'organizzazione sta utilizzando. |
| `Ultimo aggiornamento` | Data e ora più recenti in cui Salesforce ha scattato un'istantanea dell'utilizzo della risorsa da parte dell'organizzazione. |

Per ulteriori informazioni sulle risorse a cui ha diritto l'organizzazione, rivolgersi a Salesforce.

VEDERE ANCHE:

Panoramica sui diritti basati sull'utilizzo

Visualizzazione dei diritti basati sull'utilizzo dell'organizzazione

# Password

L'amministratore può configurare varie impostazioni per garantire che le password degli utenti siano sicure ed efficaci.

- Criteri relativi alle password: impostare diversi criteri relativi alle password e all'accesso, ad esempio specificare un periodo di tempo entro il quale le password di tutti gli utenti scadono e il livello di complessità richiesto per le password. Vedere Impostazione dei criteri relativi alle password a pagina 183.
- Scadenza delle password degli utenti: impostare la scadenza delle password di tutti gli utenti dell'organizzazione, ad eccezione di quelli che dispongono dell'autorizzazione "La password non ha scadenza". Vedere Impostazione di una scadenza per le password utente a pagina 187.
- Reimpostazioni delle password degli utenti: ripristinare le password di utenti specifici. Vedere Reimpostazione delle password per gli utenti a pagina 186.
- Tentativi di accesso e periodi di blocco: se un utente non riesce più ad accedere a Salesforce a causa dei troppi tentativi di accesso non riusciti, è possibile sbloccarlo. Vedere Modifica degli utenti a pagina 139.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Criteri relativi alle password disponibili in: **tutte** le versioni

AUTORIZZAZIONI UTENTE

Per impostare i criteri di password:
- "Gestisci criteri relativi alle password"

Per reimpostare le password degli utenti e sbloccare gli utenti:
- "Reimposta password utente e sblocca utenti"

## Requisiti delle password

Una password non può contenere il nome utente e non può essere uguale al nome o al cognome di un utente. Inoltre, le password non possono essere troppo semplici. Ad esempio, un utente non può cambiare la password in `password`.

Per tutte le versioni, le password impostate da una nuova organizzazione devono soddisfare i seguenti requisiti predefiniti. I criteri per le password si possono modificare in tutte le versioni, tranne la versione Personal Edition.

- Una password deve contenere almeno otto caratteri, compreso un carattere alfabetico e un numero.
- La risposta alla domanda di sicurezza non può contenere la password dell'utente.
- Quando modificano la password, gli utenti non possono riutilizzare le ultime tre password.

## Impostazione dei criteri relativi alle password

Per la sicurezza dell'organizzazione, è possibile impostare vari criteri per le password e l'accesso.

Nota: le password degli utenti non possono superare i 16.000 byte.

Gli accessi sono limitati a 3.600 ore per utente. Questo limite si applica alle organizzazioni create dopo il rilascio Summer '08.

1. Da Imposta, immettere *Criteri relativi alle password* nella casella Ricerca veloce, quindi selezionare **Criteri relativi alle password**.
2. Personalizzare le impostazioni relative alle password.

| Campo | Descrizione |
|---|---|
| Le password utente scadono tra | Periodo di tempo al termine del quale tutte le password utente scadono e devono essere cambiate. Questa impostazione non si applica agli utenti in possesso dell'autorizzazione "La password non ha scadenza". Il valore predefinito è 90 giorni. Questa impostazione non è disponibile per i portali Self-Service. |
| Memorizza le ultime password | Consente di salvare le password precedenti degli utenti in modo che occorra sempre reimpostarle su un valore nuovo e univoco. La cronologia delle password non viene salvata finché non si imposta questo valore. Il valore predefinito è 3 password memorizzate. Non è possibile selezionare l'opzione Nessuna password memorizzata a meno che per il campo Le password utente scadono tra non sia stata selezionata l'opzione Nessuna scadenza. Questa impostazione non è disponibile per i portali Self-Service. |
| Lunghezza minima password | Numero minimo di caratteri richiesti per una password. L'impostazione di questo valore non ha effetto sugli utenti esistenti finché non cambiano la propria password. Il valore predefinito è 8 caratteri. |
| Requisito di complessità password | Requisito relativo ai tipi di caratteri che gli utenti possono utilizzare in una password.<br>Livelli di complessità:<br>• Nessuna limitazione: consente qualsiasi valore della password ed è l'opzione meno sicura. |

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per impostare i criteri di password:
- "Gestisci criteri relativi alle password"

| Campo | Descrizione |
| --- | --- |
| | • `Deve contenere caratteri alfanumerici`: richiede almeno un carattere alfabetico e un numero, che corrisponde all'impostazione predefinita.<br>• `Deve contenere caratteri alfanumerici e speciali`: richiede almeno un carattere alfabetico, un numero e uno dei seguenti caratteri: `! # $ % - _ = + < >`.<br>• `Deve contenere numeri e lettere maiuscole e minuscole`: richiede almeno un numero, un carattere alfabetico maiuscolo e uno minuscolo.<br>• `Deve contenere numeri, lettere maiuscole e minuscole e caratteri speciali`: richiede almeno un numero, un carattere alfabetico maiuscolo e uno minuscolo e uno dei seguenti caratteri: `! # $ % - _ = + < >`. |
| `Requisito domanda per la password` | I valori sono di tipo `Non può contenere la password`, ovvero la risposta alla domanda di suggerimento della password non può contenere la password, oppure di tipo `Nessuna`, l'impostazione predefinita, se non vi sono limitazioni relative alla risposta. È richiesta la risposta dell'utente alla domanda di suggerimento della password. Questa impostazione non è disponibile per i portali Self-Service, i Portali Clienti o i portali partner. |
| `Numero massimo di tentativi di accesso non validi` | Numero di accessi non riusciti consentiti a un utente prima che venga bloccato. Questa impostazione non è disponibile per i portali Self-Service. |
| `Periodo effettivo di blocco` | Durata del blocco dell'accesso. Il valore predefinito è 15 minuti. Questa impostazione non è disponibile per i portali Self-Service.<br>Nota: gli utenti il cui accesso è stato bloccato, devono aspettare la scadenza del periodo di blocco. In alternativa, un utente con l'autorizzazione "Reimposta password utente e sblocca utenti" può sbloccarli facendo clic su *Utenti* nella casella `Ricerca veloce`, quindi selezionando **Utenti**, selezionando l'utente e facendo clic su **Sblocca**. Questo pulsante è disponibile solo quando un utente è bloccato. |
| `Oscura risposta segreta per le reimpostazioni delle password` | Questa funzione consente di nascondere le risposte alle domande di sicurezza durante la digitazione. L'impostazione predefinita mostra la risposta come testo normale.<br>Nota: se l'organizzazione utilizza l'IME (Input Method Editor) Microsoft con la modalità di inserimento impostata su Hiragana, quando si digitano i caratteri ASCII essi |

| Campo | Descrizione |
| --- | --- |
| | vengono convertiti in caratteri giapponesi nei campi di testo normale. Tuttavia, l'IME non funziona correttamente nei campi con testo oscurato. Se gli utenti dell'organizzazione non riescono a immettere correttamente le loro password o altri valori dopo l'abilitazione di questa funzione, disabilitarla. |
| `Richiedi una durata della password di almeno 1 giorno` | Quando si seleziona questa opzione, una password non può essere modificata più di una volta nell'arco di 24 ore. |

3. Personalizzare le informazioni di assistenza in caso di password dimenticata e account bloccato.

   Nota: Questa impostazione non è disponibile per i portali Self-Service, i Portali Clienti o i portali partner.

| Campo | Descrizione |
| --- | --- |
| `Messaggio` | Se impostato, questo messaggio viene visualizzato nel messaggio email "Non siamo in grado di reimpostare la password" che gli utenti ricevono quando si sbloccano tentando troppe volte di reimpostare la password. Il testo viene visualizzato anche in fondo alla pagina Digita la risposta alla domanda di sicurezza quando gli utenti reimpostano le loro password.<br><br>È possibile personalizzare il testo per la propria organizzazione aggiungendo il nome del proprio help desk interno o di un amministratore di sistema. Nel caso del messaggio email, questo messaggio viene visualizzato esclusivamente per gli account che devono essere reimpostati da un amministratore di sistema. Per i blocchi dovuti a limitazioni di tempo, viene inviato un messaggio email di sistema diverso. |
| `Link della Guida` | Se è impostato, questo link visualizza il testo definito nel campo `Messaggio`. Nel messaggio email "Non siamo in grado di reimpostare la password", l'URL viene visualizzato come è stato digitato nel campo `Link della Guida`, in modo che l'utente possa vedere la destinazione del link. Il formato di visualizzazione di questo URL costituisce una misura di sicurezza, in quanto l'utente non è all'interno di un'organizzazione Salesforce.<br><br>Nella pagina "Digita la risposta alla domanda di sicurezza", l'URL `Link della Guida` viene associato al testo contenuto nel campo `Messaggio` in modo da generare un link cliccabile. In questo caso la sicurezza non è un problema, perché l'utente è all'interno di un'organizzazione Salesforce quando cambia la propria password.<br><br>Protocolli validi: |

| Campo | Descrizione |
| --- | --- |
| | • http<br>• https<br>• mailto |

4. Specificare una pagina iniziale alternativa per gli utenti con l'autorizzazione "Utente solo API". Dopo che hanno completato le operazioni di gestione utente, quali la reimpostazione di una password, gli utenti solo API vengono reindirizzati all'URL specificato qui e non alla pagina di accesso.
5. Fare clic su **Salva**.

VEDERE ANCHE:

Password

## Reimpostazione delle password per gli utenti

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per reimpostare password:
- "Reimposta password utente e sblocca utenti"

Gli amministratori possono reimpostare la password di un utente per migliorare la sicurezza, oppure per sbloccare un utente che è stato bloccato.

Per reimpostare la password di un utente:

1. Da Imposta, immettere *Utenti* nella casella `Ricerca veloce`, quindi selezionare **Utenti**.
2. Selezionare la casella di controllo accanto al nome dell'utente. Se lo si desidera, per modificare le password di tutti gli utenti correntemente visualizzati selezionare la casella nell'intestazione della colonna per selezionare tutte le righe.
3. Fare clic su **Reimposta password**. L'utente riceve un'email che contiene un link e le istruzioni per reimpostare la password.

Una password creata in questo modo non scade, ma gli utenti devono modificarla la prima volta che eseguono l'accesso.

Suggerimento: questa e altre operazioni di amministrazione possono essere eseguite dall'app mobile SalesforceA.

### Considerazioni per la reimpostazione delle password

- Solo un amministratore può reimpostare le password degli utenti con Single Sign-On. Gli utenti con Single Sign-On non possono reimpostare la propria password.
- Dopo avere reimpostato una password, è possibile che gli utenti debbano attivare i computer per poter accedere correttamente a Salesforce.
- La reimpostazione della password di un utente bloccato ne sblocca automaticamente anche l'account.
- Quando dimentica una password, l'utente può fare clic sul link Password dimenticata nella pagina di accesso per ricevere un'email contenente le istruzioni per reimpostare la password. Per reimpostare la password, l'utente deve rispondere correttamente alla domanda di sicurezza. In Criteri relativi alle password è possibile personalizzare la pagina della domanda di sicurezza visualizzata dall'utente con informazioni su come ottenere assistenza.

Nota: se l'utente non ha impostato una domanda di sicurezza o non risponde correttamente alla domanda, la password non viene reimpostata.

L'utente può richiedere di reimpostare la password tramite il link Password dimenticata per un massimo di cinque volte nell'arco di 24 ore. Gli amministratori possono reimpostare le password degli utenti ogni volta che è necessario.

- Con la reimpostazione della password viene reimpostato anche il token di protezione dell'utente.

VEDERE ANCHE:

Password

SalesforceA

## Impostazione di una scadenza per le password utente

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per impostare la scadenza di tutte le password:

- "Gestisci utenti interni"

Un amministratore può impostare la scadenza delle password di tutti gli utenti ogni volta che si desidera rafforzare la protezione nell'organizzazione.

Per impostare la scadenza delle password di tutti gli utenti, ad eccezione di quelli che dispongono dell'autorizzazione "La password non ha scadenza":

1. Da Imposta, immettere *Scadenza di tutte le password* nella casella Ricerca veloce, quindi selezionare **Scadenza di tutte le password**.
2. Selezionare **Scadenza di tutte le password utente**.
3. Fare clic su **Salva**.

Al successivo accesso, agli utenti verrà richiesto di reimpostare la password.

### Considerazioni sulla scadenza delle password

- È possibile che gli utenti debbano attivare i propri computer per accedere a Salesforce.
- L'opzione Scadenza di tutte le password utente non ha alcun effetto sugli utenti del portale Self-Service, in quanto non sono utenti diretti di Salesforce.

VEDERE ANCHE:

Password

# Controllo dell'accesso

1. Da Imposta, immettere `Criteri di accesso` nella casella `Ricerca veloce`, quindi selezionare **Criteri di accesso**.
2. Per consentire a un amministratore di accedere in veste di qualsiasi utente dell'organizzazione senza prima chiedere all'utente che gli conceda l'accesso, abilitare **Gli amministratori possono accedere sotto forma di qualsiasi utente**. Questa opzione potrebbe essere già abilitata per impostazione predefinita. Per disabilitare l'opzione, deselezionare la casella di controllo `Abilitato`.

   Per rimuovere questa funzionalità dall'organizzazione, contattare Salesforce.
3. Per impedire agli utenti di concedere l'accesso a un autore pubblicazione (ad esempio per motivi di regolamentazione o riservatezza), fare clic su **Disponibile solo agli amministratori** per quell'autore pubblicazione.
4. Fare clic su **Salva**.

Tenere presenti queste limitazioni di implementazione.

- Gli utenti non possono concedere accesso ai pacchetti gestiti concessi in licenza a tutta l'organizzazione. Solo gli amministratori con l'autorizzazione “Gestisci utenti” abilitata nel loro profilo possono concedere accesso a questi autori pubblicazione.
- L'accesso è disponibile solo per alcuni pacchetti gestiti. Se il pacchetto non è presente nell'elenco, non è disponibile per la concessione dell'accesso.
- Se si disabilita l'opzione **Gli amministratori possono accedere sotto forma di qualsiasi utente** o se si chiede a Salesforce di rimuovere la funzionalità dall'organizzazione, un utente deve concedere l'accesso affinché l'amministratore possa accedere all'account di quell'utente per risolvere i problemi.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

La concessione dell'accesso amministratore è disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per controllare i criteri di accesso:

- "Gestisci criteri di accesso"

VEDERE ANCHE:

Accesso come un altro utente

## Accesso come un altro utente

Per fornire assistenza agli altri utenti, gli amministratori possono effettuare l'accesso a Salesforce come un altro utente. A seconda delle impostazioni dell'organizzazione, i singoli utenti potrebbero dover prima concedere l'accesso agli amministratori.

Nota: Come misura di sicurezza, quando gli amministratori sono registrati come un altro utente, non possono autorizzare l'accesso ai dati OAuth per quell'utente. Ad esempio, gli amministratori non possono autorizzare l'accesso OAuth agli account utente, incluso il Single Sign-On alle applicazioni di terze parti.

1. Da Imposta, digitare `Utenti` nella casella `Ricerca veloce`, quindi selezionare **Utenti**.
2. Fare clic sul link **Accesso** accanto al nome dell'utente. Questo link è disponibile solo per gli utenti che hanno concesso l'accesso a un amministratore o nelle organizzazioni in cui gli amministratori possono accedere come qualsiasi utente.
3. Per ritornare all'account di amministratore, fare clic su `Nome utente` > **Esci**.

VEDERE ANCHE:

Controllo dell'accesso

Visualizzazione e gestione degli utenti

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per effettuare l'accesso come un altro utente:
- "Modifica tutti i dati"

# Delega delle funzioni amministrative

Utilizzare l'amministrazione delegata per assegnare privilegi amministrativi limitati agli utenti dell'organizzazione che non sono amministratori.

Gli amministratori delegati possono:

- Creare e modificare gli utenti in ruoli specifici e in tutti i ruoli subordinati. Le operazioni di modifica degli utenti includono la reimpostazione delle password, l'impostazione delle quote, la creazione di team opportunità predefiniti e la creazione di gruppi personali per quegli utenti
- Sbloccare gli utenti
- Assegnare gli utenti a specifici profili e insiemi di autorizzazioni
- Creare gruppi pubblici e gestire l'appartenenza in gruppi pubblici specifici
- Effettuare l'accesso come utenti che abbiano concesso il diritto di accesso all'amministratore
- Gestire oggetti personalizzati

Ad esempio, si supponga di volere che il responsabile del team di assistenza gestisca gli utenti nel ruolo Responsabile assistenza e in tutti i ruoli subordinati. La creazione di un amministratore delegato a questo scopo consente all'amministratore di sistema di concentrarsi su altre operazioni di amministrazione.

Per creare gruppi delegati, da Imposta, immettere `Amministrazione delegata` nella casella `Ricerca veloce`, quindi selezionare **Amministrazione delegata** e fare clic su **Nuova**.

Nota:

- Quando gli amministratori delegati vengono assegnati a più gruppi delegati, possono amministrare gli utenti in tutti questi gruppi delegati. Ad esempio, si supponga che Mario Rossi venga specificato come amministratore in due gruppi delegati, il Gruppo A e il

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per gestire l'amministrazione delegata:
- "Personalizza applicazione"

Per diventare amministratore delegato:
- "Visualizza impostazione e configurazione"

Gruppo B. Mario può assegnare un insieme di autorizzazioni o un gruppo pubblico dal Gruppo A agli utenti nel Gruppo B.

- per delegare l'amministrazione di oggetti specifici, utilizzare le autorizzazioni relative agli oggetti, quali "Visualizza tutto" e "Modifica tutto".

VEDERE ANCHE:

Definizione di amministratori delegati

Delega dell'amministrazione degli utenti

Delega di assegnazione di insiemi di autorizzazioni

Delega dell'amministrazione di oggetti personalizzati

## Definizione di amministratori delegati

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per gestire l'amministrazione delegata:

- "Personalizza applicazione"

Per diventare amministratore delegato:

- "Visualizza impostazione e configurazione"

Un gruppo di amministratori delegati è un gruppo formato da utenti dotati dei medesimi privilegi di amministratore. Tali gruppi non sono correlati ai gruppi pubblici utilizzati per la condivisione.

1. Da Imposta, immettere *`Amministrazione delegata`* nella casella `Ricerca veloce`, quindi selezionare **Amministrazione delegata**.
2. Fare clic su **Nuovo**.
3. Immettere il nome di un gruppo.
4. Per consentire agli utenti di questo gruppo di accedere in qualità di utenti appartenenti alla gerarchia dei ruoli che amministrano, selezionare **Abilita gruppo per l'accesso**. A seconda delle impostazioni della propria organizzazione, è possibile che i singoli utenti debbano concedere l'accesso ai rispettivi amministratori.
5. Fare clic su **Salva**.
6. Per specificare gli utenti presenti in questo gruppo delegato, fare clic su **Aggiungi** nell'elenco correlato Amministratori delegati.
7. Fare clic su per trovare gli utenti e aggiungerli al gruppo. Gli utenti devono disporre dell'autorizzazione "Visualizza impostazione e configurazione".
8. Fare clic su **Salva**.

VEDERE ANCHE:

Delega delle funzioni amministrative

# Delega dell'amministrazione degli utenti

È possibile abilitare amministratori delegati per gestire utenti in ruoli specifici e in tutti i ruoli subordinati, per assegnare profili specifici a tali utenti ed effettuare l'accesso in qualità di utenti che hanno concesso l'accesso agli amministratori.

1. Da Imposta, immettere *Amministrazione delegata* nella casella `Ricerca veloce`, quindi selezionare **Amministrazione delegata**.
2. Selezionare o creare un gruppo delegato.
3. Fare clic su **Aggiungi** nell'elenco correlato Amministrazione utenti.
4. Fare clic su  per trovare e aggiungere i ruoli. Gli amministratori delegati possono creare e modificare utenti in tali ruoli e in tutti i ruoli subordinati.
5. Fare clic su **Salva**.
6. Fare clic su **Aggiungi** nell'elenco correlato Profili assegnabili.
7. Fare clic su  per trovare e aggiungere i profili. Gli amministratori delegati possono assegnare tali profili agli utenti da loro creati e modificati.

   Nota:

   - Gli amministratori delegati non possono assegnare profili o insiemi di autorizzazioni con l'autorizzazione "Modifica tutti i dati".
   - Gli amministratori delegati che fanno parte di più gruppi di amministratori delegati possono assegnare qualsiasi profilo assegnabile a tutti gli utenti nei ruoli che possono gestire.

8. Fare clic su **Salva**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per gestire l'amministrazione delegata:

- "Personalizza applicazione"

Per diventare amministratore delegato:

- "Visualizza impostazione e configurazione"

VEDERE ANCHE:

Delega di assegnazione di insiemi di autorizzazioni

Delega dell'amministrazione di oggetti personalizzati

Delega delle funzioni amministrative

## Delega di assegnazione di insiemi di autorizzazioni

Abilitare amministratori delegati per l'assegnazione di insiemi di autorizzazioni agli utenti in ruoli specifici e in tutti i ruoli subordinati.

Gli amministratori delegati non possono modificare gli insiemi di autorizzazioni. Possono solo assegnare o rimuovere gli insiemi di autorizzazioni degli utenti nei loro gruppi.

1. Da Imposta, immettere *Amministrazione delegata* nella casella Ricerca veloce, quindi selezionare **Amministrazione delegata**.
2. Selezionare un gruppo di amministratori delegati o crearne uno.
3. Dalla pagina dei dettagli del gruppo di amministratori delegati, fare clic su **Modifica** nell'elenco correlato Insiemi di autorizzazioni assegnabili.
4. Specificare gli insiemi di autorizzazioni che gli amministratori delegati di questo gruppo possono assegnare agli utenti.
5. Fare clic su **Salva**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per gestire l'amministrazione delegata:
- "Personalizza applicazione"

Per diventare amministratore delegato:
- "Visualizza impostazione e configurazione"

VEDERE ANCHE:

Delega delle funzioni amministrative

## Gestione delegata gruppi pubblici

Abilitare amministratori delegati alla creazione di gruppi pubblici e all'aggiunta e rimozione di utenti in gruppi pubblici specificati.

1. Da Imposta, immettere *Amministrazione delegata* nella casella Ricerca veloce, quindi selezionare **Amministrazione delegata**.
2. Selezionare un gruppo di amministratori delegati o crearne uno.
3. Dalla pagina dei dettagli del gruppo di amministratori delegati, fare clic su **Modifica** nell'elenco correlato Gruppi pubblici assegnabili.
4. Specificare i gruppi pubblici che gli amministratori delegati di questo gruppo possono gestire.

   Per i gruppi pubblici che vengono specificati, gli amministratori delegati potranno aggiungere e rimuovere utenti nei loro ruoli specificati e nei ruoli subordinati.
5. Fare clic su **Salva**.

VEDERE ANCHE:

Delega delle funzioni amministrative

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per gestire l'amministrazione delegata:

- "Personalizza applicazione"

Per diventare amministratore delegato:

- "Visualizza impostazione e configurazione"

# Delega dell'amministrazione di oggetti personalizzati

Abilitare amministratori delegati per la gestione degli oggetti personalizzati.

1. Da Imposta, immettere *Amministrazione delegata* nella casella Ricerca veloce, quindi selezionare **Amministrazione delegata**.
2. Selezionare il nome di un gruppo di amministrazione delegati esistente.
3. Dalla pagina dei dettagli del gruppo di amministratori delegati, fare clic su **Aggiungi** nell'elenco correlato Amministrazione oggetti personalizzati.
4. Utilizzare l'icona di ricerca (lente di ingrandimento) per individuare e aggiungere oggetti personalizzati. Gli amministratori delegati possono personalizzare quasi tutti gli aspetti di un oggetto personalizzato, inclusa la creazione di una scheda personalizzata per l'oggetto.
5. Fare clic su **Salva**. Fare clic su **Salva e Altro** per aggiungere altri oggetti personalizzati.

Per rimuovere un oggetto personalizzato dall'elenco degli elementi che gli amministratori delegati possono gestire, fare clic su **Rimuovi** accanto all'oggetto personalizzato.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per gestire l'amministrazione delegata:
- "Personalizza applicazione"

Per diventare amministratore delegato:
- "Visualizza impostazione e configurazione"

## Note sulla delega dell'amministrazione di oggetti personalizzati

- Gli amministratori delegati possono personalizzare quasi tutti gli aspetti dell'oggetto personalizzato, inclusa la creazione di una scheda personalizzata per l'oggetto. Tuttavia, non possono creare o modificare relazioni dell'oggetto o stabilire impostazioni predefinite di condivisione dell'organizzazione.
- Gli amministratori delegati devono avere accesso agli oggetti personalizzati se devono accedere ai campi di unione di tali oggetti dalle formule.

VEDERE ANCHE:

Delega delle funzioni amministrative

# Impostazioni di argomenti e tag

Con o senza Chatter abilitato, gli amministratori possono abilitare gli argomenti per gli oggetti e consentire agli utenti di aggiungere gli argomenti ai record, in modo tale che possano recuperare rapidamente gli elementi correlati utilizzando le visualizzazioni elenco. Con Chatter abilitato, gli utenti possono inoltre visualizzare gli elementi correlati nella scheda Record della pagina dei dettagli di ogni argomento. Abilitando gli argomenti per un oggetto, si disabilitano i tag pubblici dei record per quel tipo di oggetto. L'operazione non influisce sui tag personali.

Per utilizzare gli argomenti per organizzare i record, abilitare gli argomenti per account, asset, campagne, casi, referenti, contratti, lead, opportunità, ordini, soluzioni e oggetti personalizzati.

Gli amministratori configurano e gestiscono i tag personali e pubblici:

- Abilitando i tag per account, attività, asset, campagne, casi, referenti, contratti, cruscotti digitali, documenti, eventi, lead, note, opportunità, rapporti, soluzioni, operazioni e qualsiasi oggetto personalizzato
- Aggiungendo i tag all'intestazione laterale per gli utenti
- Eliminando i tag personali degli utenti disattivati

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Le impostazioni per argomenti e tag sono disponibili in: **tutte** le versioni

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni di argomenti e tag:
- "Personalizza applicazione"

## Abilitazione e configurazione degli argomenti per gli oggetti

Abilitare gli argomenti per gli oggetti in modo tale che gli utenti possano aggiungere argomenti ai record e organizzarli in base a temi comuni. Questa potente funzionalità è disponibile con o senza Chatter.

Gli amministratori possono abilitare gli argomenti per account, asset, campagne, casi, referenti, contratti, lead, opportunità, ordini, soluzioni e oggetti personalizzati. Per ogni tipo di oggetto, gli amministratori specificano quali campi utilizzare per i suggerimenti sugli argomenti.

Avvertenza: quando sono abilitati gli argomenti per un oggetto, i tag pubblici vengono disabilitati per i record di quel tipo di oggetto.

1. Da Imposta, immettere *Argomenti per gli oggetti* nella casella Ricerca veloce, quindi selezionare **Argomenti per gli oggetti**.
2. Selezionare un oggetto.
3. A destra, selezionare Abilita argomenti.
4. Selezionare i campi di testo che si desidera utilizzare per i suggerimenti sugli argomenti. (Da una combinazione dei campi selezionati, vengono formulati fino a 3 suggerimenti tra i primi 2.000 caratteri).
5. Fare clic su **Salva** per salvare le modifiche per tutti gli oggetti.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **tutte** le versioni

AUTORIZZAZIONI UTENTE

Per abilitare gli argomenti per gli oggetti:
- "Personalizza applicazione"

A questo punto, gli utenti che dispongono dell'accesso agli oggetti abilitati e delle autorizzazioni appropriate sugli argomenti possono:

- Vedere le assegnazioni degli argomenti e i suggerimenti sui record di quel tipo di oggetto
- Aggiungere ed eliminare argomenti dai record su quel tipo di oggetto
- Utilizzare gli argomenti sui record di quel tipo di oggetto per filtrare le loro visualizzazioni elenco

Inoltre, se l'organizzazione utilizza Chatter, gli utenti possono fare clic su qualsiasi argomento assegnato a un record per accedere direttamente alla pagina di un argomento, dove troveranno altri record sull'argomento, le persone esperte sull'argomento e altre informazioni correlate.

## Abilitazione di tag

1. Da Imposta, immettere *Impostazioni tag* nella casella Ricerca veloce, quindi selezionare **Impostazioni tag**.
2. Selezionare Abilita tag personali e Abilita tag pubblici per consentire agli utenti di aggiungere tag personali e pubblici ai record. Deselezionare entrambe le opzioni per disabilitare i tag.
3. Specificare gli oggetti e i layout di pagina che devono visualizzare i tag in una sezione dei tag nella parte superiore delle pagine dei dettagli dei record. La sezione dei tag rappresenta l'unico modo che un utente ha a disposizione per aggiungere tag a un record.

   Ad esempio, se si selezionano solo i layout di pagina di account, gli utenti dell'organizzazione possono creare tag solo per i record di account. Inoltre, se si selezionano solo i layout di pagina di account per i tag personali e non per i tag pubblici, gli utenti possono solo assegnare tag personali ai record account.
4. Fare clic su **Salva**.

Quando si abilitano i tag, tenere presenti queste linee guida.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Le impostazioni dei tag sono disponibili in: **tutte** le versioni

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni dei tag:
- "Personalizza applicazione"

- È possibile anche aggiungerli ai layout di pagina modificando un layout direttamente. Tenere presente, tuttavia, che i tag non possono essere aggiunti ai layout di pagina basati su feed.
- I risultati delle ricerche e la pagina Tag non visualizzano gli oggetti personalizzati a cui non è associata una scheda, anche se i tag sono abilitati per l'oggetto personalizzato. Per far sì che vengano visualizzati i record degli oggetti personalizzati, creare una scheda associata. Non è necessario che la scheda sia visibile agli utenti.
- Gli utenti del Portale Clienti non possono visualizzare la sezione dei tag di una pagina, anche se viene inclusa in un layout di pagina.
- Quando Chatter è disabilitato non è possibile creare tag per i rapporti uniti.

VEDERE ANCHE:

Impostazioni di argomenti e tag

## Aggiunta di tag all'intestazione laterale

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Le impostazioni dei tag sono disponibili in: **tutte** le versioni

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni dei tag:
- "Personalizza applicazione"

Quando si abilitano i tag per l'organizzazione, è possibile aggiungere il componente Tag all'intestazione laterale degli utenti. Questo componente consente agli utenti di spostarsi sulla pagina Tag dalla quale possono sfogliare, cercare e gestire i loro tag. Inoltre, vengono qui elencati gli ultimi tag utilizzati dall'utente. Per aggiungere questo componente:

1. Da Imposta, immettere *`Layout pagina iniziale`* nella casella `Ricerca veloce`, quindi selezionare **Layout pagina iniziale**.
2. Fare clic su **Modifica** accanto al layout di pagina iniziale che si desidera modificare.
3. Selezionare la casella di controllo `Tag` e fare clic su **Avanti**.
4. Posizionare il componente Tag sul layout di pagina in base alle proprie esigenze e fare clic su **Salva**.

Suggerimento: per fare in modo che il componente Tag appaia in tutte le pagine e non solo nella scheda Pagina iniziale, fare clic su *`Interfaccia utente`* nella casella `Ricerca veloce`, quindi selezionare **Interfaccia utente** e selezionare `Mostra componenti intestazione laterale personalizzata in tutte le pagine`.

VEDERE ANCHE:

Impostazioni di argomenti e tag

## Eliminazione di tag personali per gli utenti disattivati

L'organizzazione può applicare ai record fino a un massimo di 5.000.000 di tag personali e pubblici tra tutti gli utenti. Se l'organizzazione si avvicina al limite, è possibile eliminare i tag personali degli utenti disattivati.

1. Da Imposta, immettere *Pulitura tag personali* nella casella Ricerca veloce, quindi selezionare **Pulitura tag personali**.
2. Selezionare uno o più utenti disattivati e fare clic su **Elimina**.

I tag personali eliminati non possono essere ripristinati.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Pulitura tag personali disponibile in: **tutte** le versioni

AUTORIZZAZIONI UTENTE

Per eliminare tag personali per gli utenti disattivati:

- "Personalizza applicazione"

VEDERE ANCHE:

Impostazioni di argomenti e tag

# Gestione dell'accesso ai dati da parte degli utenti

## Protezione dell'accesso ai dati

Una delle scelte chiave che incidono sulla sicurezza dei dati è la scelta dell'insieme di dati che ciascun utente o gruppo di utenti può visualizzare. È necessario trovare un compromesso tra la limitazione dell'accesso ai dati, per ridurre il rischio di furto o uso errato, e la comodità dell'accesso ai dati per gli utenti.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Le opzioni di gestione dei dati disponibili variano a seconda della versione di Salesforce utilizzata.

Per consentire agli utenti di svolgere il loro lavoro senza esporre dati che non hanno bisogno di visualizzare, Salesforce fornisce una struttura di condivisione flessibile su più livelli che consente di esporre diversi insiemi di dati a diversi gruppi di utenti.

- Per specificare gli oggetti a cui gli utenti possono accedere, è possibile assegnare insiemi di autorizzazioni e profili.
- Per specificare i campi a cui gli utenti possono accedere, è possibile utilizzare la protezione a livello di campo.
- Per specificare i singoli record che gli utenti possono visualizzare e modificare, è possibile definire le impostazioni di condivisione valide per tutta l'organizzazione, definire una gerarchia dei ruoli e creare regole di condivisione.

Suggerimento: quando si implementano le regole di protezione e condivisione per la propria organizzazione, creare una tabella dei diversi tipi di utenti della propria organizzazione. Nella tabella, specificare il livello di accesso ai dati che ciascun tipo di utente necessita per ciascun oggetto e per i campi e i record di quell'oggetto. Questa tabella tornerà utile quando si configura il proprio modello di protezione.

Di seguito sono descritte le impostazioni di protezione e di condivisione:

**Protezione a livello di oggetto (insiemi di autorizzazioni e profili)**

La protezione a livello di oggetto (autorizzazioni oggetti) rappresenta il modo più diretto per controllare i dati. Con le autorizzazioni oggetti è possibile impedire a un utente di visualizzare, creare, modificare o eliminare le istanze di un determinato tipo di oggetto, ad esempio un lead o un'opportunità. Le autorizzazioni oggetti consentono di nascondere completamente schede e oggetti per determinati utenti, in modo tale che non sappiano nemmeno che quel tipo di dati esiste.

È possibile specificare le autorizzazioni oggetti negli insiemi di autorizzazioni e nei profili. *Gli insiemi di autorizzazioni* e i *profili* sono raccolte di impostazioni e autorizzazioni che determinano quali operazioni può eseguire un utente nell'applicazione, come un gruppo in una rete Windows, dove tutti i membri del gruppo hanno le stesse autorizzazioni cartella e il medesimo accesso allo stesso software.

I profili normalmente si definiscono in base alla qualifica di un utente, ad esempio amministratore di sistema o agente di vendita. Un profilo può essere assegnato a molti utenti, ma un utente può essere assegnato a un solo profilo. È possibile utilizzare gli insiemi di autorizzazioni per concedere ulteriori autorizzazioni e impostazioni di accesso agli utenti. La gestione delle autorizzazioni e dell'accesso con insiemi di autorizzazioni degli utenti è semplice, poiché è possibile assegnare più insiemi di autorizzazioni a un solo utente.

**Protezione a livello di campo (insiemi di autorizzazioni e profili)**

In alcuni casi, è opportuno fare in modo che gli utenti possano accedere a un oggetto, limitando però il loro accesso a singoli campi di tale oggetto. La protezione a livello di campo (autorizzazioni campi) consente di stabilire se un utente può visualizzare, modificare ed eliminare il valore di un determinato campo su un oggetto. Consente inoltre di proteggere i campi più critici senza nascondere l'intero oggetto agli utenti. Le autorizzazioni campi possono essere controllate anche negli insiemi di autorizzazioni e nei profili.

A differenza dei layout di pagina, che controllano solo la visibilità dei campi nelle pagine dei dettagli e di modifica, le autorizzazioni campi controllano la visibilità dei campi in qualsiasi parte dell'applicazione, inclusi gli elenchi correlati, le visualizzazioni elenco, i rapporti e i risultati della ricerca. Per assicurarsi che un utente non possa accedere a un determinato campo, utilizzare le autorizzazioni campi. Nessun'altra impostazione fornisce lo stesso livello di protezione per un campo.

Nota: La protezione a livello di campo non impedisce di effettuare ricerche sui valori di un campo. Quando i termini della ricerca corrispondono ai valori di campo con protezione a livello di campo, nei risultati della ricerca vengono restituiti i record associati senza i campi protetti e i relativi valori.

**Protezione livello record (Condivisione)**

Dopo avere impostato le autorizzazioni per l'accesso a livello di oggetto e di campo, devono essere configurate le impostazioni di accesso per i record. La protezione livello di record consente di fornire agli utenti l'accesso ad alcuni record oggetti, ma non ad altri. Ogni record è di proprietà di un utente o di un'area di attesa. Il titolare ha pieno accesso al record. In una gerarchia, gli utenti di livello gerarchico superiore dispongono sempre dell'accesso ai record a cui accedono gli utenti dei livelli inferiori. Questo accesso vale per i record di proprietà degli utenti e per i record condivisi con gli utenti.

Per specificare la protezione livello record, definire le impostazioni di condivisione valide per tutta l'organizzazione, definire una gerarchia e creare le regole di condivisione:

- Impostazioni di condivisione dell'organizzazione: la prima fase della protezione a livello di record è determinare le impostazioni di condivisione dell'organizzazione per ciascun oggetto. Tali impostazioni specificano il livello predefinito di accesso degli utenti ai record di altri utenti.

  Utilizzare le impostazioni di condivisione dell'organizzazione per bloccare i dati al livello più restrittivo, quindi utilizzare gli altri strumenti di protezione a livello di record e di condivisione per fornire l'accesso agli altri utenti in modo selettivo. Ad esempio, si supponga che gli utenti dispongano di autorizzazioni a livello di oggetto per leggere e modificare le opportunità e che l'impostazione della condivisione a livello di organizzazione sia Sola lettura. Per impostazione predefinita, tali utenti possono leggere tutti i record opportunità, ma non possono modificarli a meno che non siano titolari del record o dispongano di autorizzazioni aggiuntive.

- Gerarchia dei ruoli: una volta specificate le impostazioni di condivisione a livello di organizzazione, il primo metodo con cui si può fornire un accesso più ampio ai record è una gerarchia dei ruoli. In modo simile all'organigramma di un'organizzazione, una gerarchia dei ruoli rappresenta un livello di accesso ai dati di cui necessita un utente o un gruppo di utenti. La gerarchia dei ruoli assicura che gli utenti ai livelli più alti dispongano sempre dell'accesso agli stessi dati a cui accedono gli utenti ai livelli inferiori della gerarchia, indipendentemente dalle impostazioni predefinite a livello di organizzazione. Non è necessario che le gerarchie dei ruoli corrispondano esattamente all'organigramma della propria organizzazione. Ciascun ruolo nella gerarchia, invece, deve rappresentare un livello di accesso ai dati di cui necessita un utente o un gruppo di utenti.

Per condividere l'accesso ai record è possibile anche utilizzare una gerarchia dei territori. Una gerarchia dei territori concede l'accesso ai record da parte degli utenti in base a criteri quali il CAP, il settore, il reddito o un campo personalizzato pertinente alla propria attività. Ad esempio, è possibile creare una gerarchia dei territori in base alla quale un utente con il ruolo "America del Nor" ha accesso a dati diversi rispetto a un utente con i ruoli "Canada" e "Stati Uniti".

> Nota: Benché sia facile confonderli, gli insiemi di autorizzazioni e i profili con ruoli controllano due elementi molto diversi. Gli insiemi di autorizzazioni e i profili controllano le autorizzazioni di accesso a oggetti e campi. I ruoli controllano principalmente l'accesso a livello di record tramite la gerarchia dei ruoli e le regole di condivisione.

- Regole di condivisione: consentono di creare eccezioni automatiche alle impostazioni di condivisione dell'organizzazione per determinati insiemi di utenti in modo da assegnare loro l'accesso ai record di cui non sono titolari o che normalmente non possono visualizzare. Le regole di condivisione, come le gerarchie dei ruoli, sono utilizzate unicamente per fornire l'accesso ai record a ulteriori utenti e non possono essere più restrittive delle impostazioni predefinite per tutta l'organizzazione.
- Condivisione manuale: talvolta non è possibile definire un gruppo omogeneo di utenti che necessitano di accesso a un particolare insieme di record. In tali situazioni, i titolari di record possono utilizzare la condivisione manuale per concedere le autorizzazioni di lettura e modifica agli utenti che altrimenti non avrebbero accesso al record in alcun modo. Benché non sia automatica come le impostazioni di condivisione dell'organizzazione, le gerarchie dei ruoli o le regole di condivisione, la condivisione manuale consente ai titolari dei record di condividere determinati record con gli utenti che ne hanno l'esigenza.
- Condivisione gestita Apex: se le regole di condivisione e la condivisione manuale non garantiscono il controllo desiderato, è possibile utilizzare la condivisione gestita Apex. La condivisione gestita Apex consente agli sviluppatori di condividere in modo programmatico gli oggetti personalizzati. Quando si utilizza la condivisione gestita Apex per condividere un oggetto personalizzato, solo gli utenti che dispongono dell'autorizzazione “Modifica tutti i dati” possono aggiungere o cambiare la condivisione sul record dell'oggetto personalizzato e l'accesso in condivisione viene mantenuto per i cambiamenti apportati dal titolare del record.

VEDERE ANCHE:

Profili

Insiemi di autorizzazioni

Panoramica sulla protezione a livello di campo

Panoramica sulle impostazioni di condivisione

# Autorizzazioni e accesso degli utenti

## Autorizzazioni e accesso degli utenti

Le autorizzazioni utente e le impostazioni di accesso sono specificate nei profili e negli insiemi di autorizzazioni. È importante capire le differenze tra i profili e gli insiemi di autorizzazioni per poterli utilizzare efficacemente.

Le operazioni che gli utenti di un'organizzazione possono eseguire sono stabilite dalle autorizzazioni e dalle impostazioni di accesso degli utenti. Le autorizzazioni, ad esempio, determinano se un utente può modificare il record di un oggetto, visualizzare il menu Imposta, svuotare il Cestino dell'organizzazione o reimpostare una password. Le impostazioni di accesso regolano altre funzioni, quali l'accesso alle classi Apex, la visibilità delle applicazioni e gli orari in cui gli utenti possono accedere.

Ogni utente dispone di un solo profilo, ma può disporre di più insiemi di autorizzazioni.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Le autorizzazioni e le impostazioni disponibili variano a seconda della versione di Salesforce utilizzata.

Per specificare l'accesso per gli utenti, utilizzare i profili per assegnare le autorizzazioni e le impostazioni di accesso minime per specifici gruppi di utenti. Quindi utilizzare gli insiemi di autorizzazioni per assegnare ulteriori autorizzazioni.

Nella tabella che segue sono riportati i tipi di autorizzazioni e le impostazioni di accesso specificate nei profili e negli insiemi di autorizzazioni.

| Tipo di autorizzazione o impostazione | Nei profili? | Negli insiemi di autorizzazioni? |
| --- | --- | --- |
| Applicazioni assegnate | ✓ | ✓ |
| Impostazioni delle schede | ✓ | ✓ |
| Assegnazioni al tipo di record | ✓ | ✓ |
| Assegnazioni al layout di pagina | ✓ | |
| Autorizzazioni oggetto | ✓ | ✓ |
| Autorizzazioni campi | ✓ | ✓ |
| Autorizzazioni utente (applicazioni e sistema) | ✓ | ✓ |
| Accesso classe Apex | ✓ | ✓ |
| Accesso alle pagine Visualforce | ✓ | ✓ |
| Accesso a fonti di dati esterne | ✓ | ✓ |
| Accesso fornitore di servizi (se Salesforce è abilitato come provider di identità) | ✓ | ✓ |
| Autorizzazioni personalizzate | ✓ | ✓ |
| Accesso client desktop | ✓ | |
| Orari di accesso | ✓ | |
| Intervalli IP di accesso | ✓ | |

VEDERE ANCHE:

Profili

Insiemi di autorizzazioni

Revoca di autorizzazioni e accesso

# Profili

Durante la creazione degli utenti, si assegna un profilo a ogni utente. I profili definiscono il modo in cui gli utenti accedono a oggetti e dati e cosa possono fare all'interno dell'applicazione.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

L'organizzazione include diversi profili standard, nei quali è possibile modificare un numero limitato di impostazioni. Nelle organizzazioni Enterprise Edition, Performance Edition, Unlimited Edition e Developer Edition, è possibile utilizzare i profili standard oppure creare profili personalizzati. Nei profili personalizzati, è possibile modificare tutte le autorizzazioni e le impostazioni ad eccezione della licenza utente. Nelle organizzazioni Contact Manager Edition, Group Edition e Professional Edition, è possibile assegnare i profili standard ai propri utenti, ma non è consentito visualizzare o modificare i profili standard e non è possibile creare profili personalizzati.

Ogni profilo appartiene esattamente a un solo tipo di licenza utente.

Salesforce dispone di due interfacce profilo. A seconda dell'interfaccia utente profilo abilitata nella propria organizzazione, è possibile:

- Visualizzare e modificare profili nell'interfaccia utente profilo ottimizzata
- Visualizzare e modificare profili nell'interfaccia utente profilo originale

VEDERE ANCHE:

Profili standard

Gestione degli elenchi di profili

Modifica di più profili con le visualizzazioni elenco profili

Autorizzazioni utente per Crittografia piattaforma

Creazione di un segreto tenant

Autorizzazioni utente per Crittografia piattaforma

Creazione di un segreto tenant

## Profili standard

Tutte le organizzazioni dispongono di profili standard che è possibile assegnare agli utenti. Nei profili standard è possibile modificare alcune impostazioni.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

I profili standard disponibili variano a seconda della versione in uso.

In ogni organizzazione sono presenti dei profili standard. Nelle versioni Enterprise Edition, Unlimited Edition, Performance Edition e Developer Edition è possibile utilizzare i profili standard oppure creare, modificare ed eliminare profili personalizzati. Nelle organizzazioni nelle quali non è possibile creare profili personalizzati (quali Contact Manager Edition, Group Edition e Professional Edition) è possibile assegnare agli utenti profili standard ma non è possibile visualizzarli o modificarli.

La tabella riportata di seguito elenca le autorizzazioni di uso comune nei profili standard.

| Nome profilo | Autorizzazioni disponibili |
|---|---|
| Amministratore del sistema | Può configurare e personalizzare l'applicazione. Ha accesso a tutte le funzionalità che non richiedono una licenza aggiuntiva. Ad esempio, gli amministratori non possono gestire le campagne a meno che non dispongano anche di una licenza Utente Marketing. Può gestire i listini prezzi e i prodotti. Può modificare le quote, ignorare/sostituire le previsioni e visualizzare qualsiasi previsione. |

| Nome profilo | Autorizzazioni disponibili |
|---|---|
| Utente piattaforma standard | Può utilizzare le applicazioni Force.com AppExchange personalizzate sviluppate nella propria organizzazione oppure installate da AppExchange. Inoltre, può utilizzare funzionalità essenziali della piattaforma come account, referenti, rapporti, cruscotti digitali, documenti e schede personalizzate. |
| Utente singolo piattaforma standard | Può utilizzare le applicazioni AppExchange personalizzate sviluppate nella propria organizzazione oppure installate da AppExchange. L'applicazione personalizzata è limitata a cinque schede. Inoltre, può utilizzare funzionalità essenziali della piattaforma come account, referenti, rapporti, cruscotti digitali, documenti e schede personalizzate. |
| Utente standard | Può creare e modificare la maggior parte dei tipi principali di record, eseguire record e visualizzare l'impostazione dell'organizzazione. Può visualizzare, ma non gestire, le campagne. Può creare, ma non rivedere, le soluzioni. Può modificare le quote personali e ignorare/sostituire le previsioni. |
| Utente Comunità Clienti | Può accedere tramite una comunità. Il suo livello di accesso a schede, oggetti e altre funzioni è determinato dalle impostazioni della comunità e dal modello di condivisione. Per ulteriori informazioni, vedere Licenze utente comunità. |
| Utente Customer Community Plus | |
| Utente Comunità Partner | |
| Utente Portale Clienti | Può autenticarsi tramite un Portale Clienti o una comunità. Può visualizzare e modificare i dati di cui è titolare diretto o i dati condivisi con utenti che hanno ruoli inferiori nella gerarchia dei ruoli del Portale Clienti; può inoltre visualizzare e modificare i casi nei quali è elencato nel campo `Nome referente`. |
| Portale clienti a volume elevato | Può autenticarsi tramite un Portale Clienti o una comunità.<br>I profili Portale Clienti a volume elevato e Sito Web autenticato sono utenti del portale a volume elevato. |
| Sito Web autenticato | |
| Responsabile Portale Clienti | Può autenticarsi tramite un Portale Clienti o una comunità. Può visualizzare e modificare i dati di cui è titolare diretto o i dati condivisi con utenti che hanno ruoli inferiori nella gerarchia dei ruoli del Portale Clienti; può inoltre visualizzare e modificare i casi nei quali è elencato nel campo `Nome referente`. |
| Utente partner | Può autenticarsi tramite un Portale partner o una comunità. |
| Responsabile soluzioni | Può rivedere e pubblicare le soluzioni. Inoltre, ha accesso alle stesse funzionalità dell'Utente standard. |
| Utente Marketing | Può gestire le campagne, importare lead, creare carte intestate, creare modelli di email in HTML, gestire documenti pubblici e aggiornare la cronologia campagne tramite le importazioni guidate. Inoltre, ha accesso alle stesse funzionalità dell'Utente standard. |

| Nome profilo | Autorizzazioni disponibili |
| --- | --- |
| Responsabili contratti | Può creare, modificare, attivare e approvare i contratti. Questo profilo può inoltre eliminare i contratti purché non siano attivati. Può modificare le quote personali e ignorare/sostituire le previsioni. |
| Sola lettura | Può visualizzare l'impostazione dell'organizzazione, eseguire ed esportare rapporti e visualizzare, ma non modificare, altri record. |
| Utente Solo Chatter | Può accedere solo a Chatter. Può accedere a tutte le persone, i profili, gruppi e i file Chatter standard. Inoltre può:<br>• Visualizzare gli account e i referenti Salesforce<br>• Utilizzare Salesforce CRM Content, Ideas e Risposte<br>• Accedere a cruscotti digitali e rapporti<br>• Utilizzare e approvare flussi di lavoro<br>• Utilizzare il calendario per creare attività e tenerne traccia<br>• Visualizzare e modificare fino a dieci oggetti personalizzati<br>• Aggiungere record ai gruppi<br>Nota: È necessario rendere visibili le schede per gli oggetti Salesforce standard a cui può accedere il profilo utente Chatter Only, in quanto per impostazione predefinita sono nascoste a questi utenti.<br>Le organizzazioni che utilizzano la versione Professional Edition devono avere abilitato i Profili per eseguire queste operazioni. Per ulteriori informazioni, contattare il proprio rappresentante Salesforce.<br>Disponibile solo con la licenza utente Chatter Only.<br>Per ulteriori informazioni sugli utenti di Chatter Plus, vedere *Chatter Plus Frequently Asked Questions*. |
| Utente Chatter Free | Può accedere solo a Chatter. Può accedere a tutte le persone, i profili, gruppi e i file Chatter standard.<br>Disponibile solo con la licenza utente Chatter Free. |
| Utente Chatter External | Può accedere solo a Chatter e ai gruppi in cui è stato invitato e interagire con i membri di quei gruppi. Disponibile solo con la licenza utente Chatter External. |
| Utente moderatore di Chatter | Può accedere solo a Chatter. Può accedere a tutte le persone, i profili, gruppi e i file Chatter standard. In aggiunta, questo utente può:<br>• Attivare e disattivare altri utenti e moderatori di Chatter Free<br>• Concedere e revocare i privilegi di moderatore<br>• Eliminare i post e i commenti che possono visualizzare |

| Nome profilo | Autorizzazioni disponibili |
| --- | --- |
| | Nota: se si cambia un profilo utente da Utente moderatore di Chatter a Utente Chatter Free, i privilegi di moderatore vengono rimossi in Chatter.<br>Disponibile solo con la licenza utente Chatter Free. |
| Utente Solo Site.com | Può accedere solo all'applicazione Site.com. Ogni utente Solo Site.com necessita inoltre di una licenza funzioni Site.com Publisher per creare e pubblicare i siti o di una licenza funzioni Site.com Contributor per modificare i contenuti.<br>In aggiunta, questo utente può:<br>• Utilizzare un'applicazione personalizzata con un massimo di 20 oggetti personalizzati<br>• Accedere all'applicazione Content, ma non agli oggetti Account e Referenti<br>• Creare un numero illimitato di schede personalizzate<br>Disponibile solo con la licenza utente Solo Site.com. |

VEDERE ANCHE:

Profili

Autorizzazioni utente

## Gestione degli elenchi di profili

Durante la creazione degli utenti, si assegna un profilo a ogni utente. I profili definiscono il modo in cui gli utenti accedono a oggetti e dati e cosa possono fare all'interno dell'applicazione. Per visualizzare i profili nell'organizzazione, da Imposta immettere *Profili* nella casella `Ricerca veloce`, quindi selezionare **Profili**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare i profili e stampare gli elenchi di profili:

- "Visualizza impostazione e configurazione"

Per eliminare le visualizzazioni elenco dei profili:

- "Gestisci profili e insiemi di autorizzazioni"

Per eliminare i profili personalizzati:

- "Gestisci profili e insiemi di autorizzazioni"

### Visualizzazione degli elenchi di profili ottimizzati

Se nell'organizzazione sono abilitate le visualizzazioni elenco di profili ottimizzate, è possibile utilizzare strumenti aggiuntivi per personalizzare, gestire e stampare gli elenchi di profili, nonché spostarsi al loro interno.

- Per mostrare un elenco filtrato di profili, selezionare una visualizzazione dall'elenco a discesa.
- Per eliminare una visualizzazione, selezionarla dall'elenco a discesa e fare clic su **Elimina**.
- Creare una visualizzazione elenco o modificare una visualizzazione esistente.
- Creare un profilo.
- Stampare la visualizzazione elenco facendo clic sull'
- Per aggiornare la visualizzazione elenco dopo averla creata o modificata, fare clic su .
- Modificare le autorizzazioni direttamente nella visualizzazione elenco.
- Per visualizzare o modificare un profilo, fare clic sul nome del profilo.
- Per eliminare un profilo personalizzato, fare clic su **Canc** accanto al relativo nome.

  Nota: non è possibile eliminare un profilo assegnato a un utente, anche se l'utente è inattivo.

### Visualizzazione dell'elenco di profili di base

- Creare un profilo.
- Per visualizzare o modificare un profilo, fare clic sul nome del profilo.
- Per eliminare un profilo personalizzato, fare clic su **Canc** accanto al relativo nome.

VEDERE ANCHE:

Modifica di più profili con le visualizzazioni elenco profili

Profili

## Creazione e modifica di visualizzazioni elenco di profili

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per creare, modificare ed eliminare visualizzazioni elenco di profili:

- "Gestisci profili e insiemi di autorizzazioni"

Se nell'organizzazione sono abilitate le visualizzazioni elenco di profili ottimizzate, è possibile creare visualizzazioni elenco di profili per mostrare un insieme di profili con i campi desiderati. Si potrebbe, ad esempio, creare una visualizzazione elenco di tutti i profili in cui è abilitata l'autorizzazione "Modifica tutti i dati".

1. Nella pagina Profili, fare clic su **Crea nuova visualizzazione** o selezionare una visualizzazione e fare clic su **Modifica**.
2. Immettere il nome della visualizzazione.
3. In Specifica i criteri di filtro, specificare le condizioni a cui gli elementi dell'elenco devono corrispondere, ad esempio `Modifica tutti i dati uguale a Vero`.
   a. Digitare il nome di un'impostazione o fare clic sull'icona di ricerca per cercare e selezionare l'impostazione desiderata.
   b. Scegliere un operatore filtro.
   c. Immettere il valore per la corrispondenza.
   d. Per specificare un'altra condizione di filtro, fare clic su **Aggiungi nuova**. È possibile specificare fino a 25 righe di condizioni di filtro.

      Per rimuovere una riga di condizione di filtro e cancellarne i valori, fare clic sull'icona di rimozione riga .
4. In Seleziona le colonne da visualizzare, specificare le impostazioni del profilo che si desidera appaiano come colonne nella visualizzazione elenco.
   a. Dall'elenco a discesa Cerca, selezionare il tipo di impostazione da ricercare.
   b. Immettere una parte o un'intera parola dell'impostazione da aggiungere e fare clic su **Trova**.

      Nota: se la ricerca trova più di 500 valori, non viene visualizzato alcun risultato. Utilizzare le fasi descritte in precedenza per perfezionare i criteri di ricerca e mostrare un numero minore di risultati.

   c. Per aggiungere o rimuovere colonne, selezionare uno o più nomi di colonne e fare clic sulla freccia **Aggiungi** o **Rimuovi**.
   d. Utilizzare le frecce **In alto**, **Su**, **Giù** e **In basso** per disporre le colonne nella sequenza desiderata.

   è possibile aggiungere fino a 15 colonne in una singola visualizzazione elenco.
5. Fare clic su **Salva** oppure, se si sta clonando una visualizzazione esistente, rinominarla e fare clic su **Salva con nome**.

VEDERE ANCHE:

Modifica di più profili con le visualizzazioni elenco profili

## Modifica di più profili con le visualizzazioni elenco profili

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per modificare più profili dalla visualizzazione elenco:
- "Gestisci profili e insiemi di autorizzazioni"

  E

  "Personalizza applicazione"

Se nell'organizzazione sono abilitate le visualizzazioni elenco di profili ottimizzate, è possibile modificare le autorizzazioni in un massimo di 200 profili direttamente dalla visualizzazione elenco, senza accedere alle singole pagine dei profili. Nelle celle modificabili compare un'icona a forma di matita ( ) quando vi si passa sopra con il mouse, mentre le celle non modificabili contengono un'icona a forma di lucchetto ( ). In alcuni casi, ad esempio nei profili standard, l'icona a forma di matita viene visualizzata ma l'impostazione non è realmente modificabile.

Avvertenza: prestare molta attenzione quando si utilizza questo metodo per modificare i profili. Poiché i profili influiscono sull'accesso fondamentale di un utente, modifiche globali potrebbe avere un effetto generale sugli utenti dell'organizzazione.

Per modificare le autorizzazioni in uno o più profili:

1. Selezionare o creare una visualizzazione elenco che includa i profili e le autorizzazioni che si desidera modificare.
2. Per modificare più profili, selezionare la casella di controllo accanto a ciascun profilo da modificare. Se si selezionano profili su più pagine, Salesforce ricorda quali sono i profili selezionati.
3. Fare doppio clic sull'autorizzazione da modificare. Per più profili, fare doppio clic sull'autorizzazione in uno dei profili selezionati.
4. Nella finestra di dialogo visualizzata, abilitare o disabilitare l'autorizzazione. In alcuni casi, la modifica di un'autorizzazione può comportare la modifica di altre autorizzazioni. Ad esempio, se "Personalizza applicazione" e "Visualizza impostazione e configurazione" sono disabilitate e si abilita "Personalizza applicazione", viene abilitata anche "Visualizza impostazione e configurazione". In tal caso la finestra di dialogo elenca le autorizzazioni interessate.
5. Per modificare più profili, selezionare **Tutti i *n* record selezionati** (dove *n* è il numero di profili selezionati).
6. Fare clic su **Salva**.

Nota:

- Per i profili standard, la modifica in linea è disponibile solo per le autorizzazioni "Single Sign-On" e "Limita per divisione".
- Se si modificano più profili, solo i profili che supportano l'autorizzazione in corso di modifica verranno modificati. Ad esempio, se si utilizza la modifica in linea per aggiungere "Modifica tutti i dati" a più profili e il profilo non dispone dell'autorizzazione "Modifica tutti i dati" a causa della licenza utente, il profilo non verrà modificato.

Se si verificano errori, viene visualizzato un messaggio che elenca tutti i profili che contengono un errore e la relativa descrizione. Fare clic sul nome del file del profilo per aprire la pagina dei dettagli del profilo. Nella finestra di errore i profili su cui si è fatto clic vengono visualizzati in testo grigio barrato.

Nota: Per visualizzare la console errori è necessario disabilitare i blocchi delle finestre pop-up nel dominio Salesforce.

Eventuali modifiche apportate vengono registrate nell'itinerario di controllo delle impostazioni.

VEDERE ANCHE:

Profili

## Clonazione di profili

Anziché creare nuovi profili, per risparmiare tempo è possibile clonare i profili esistenti e personalizzarli.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per creare i profili:
- "Gestisci profili e insiemi di autorizzazioni"

Suggerimento: se si clonano i profili per abilitare alcune autorizzazioni o impostazioni di accesso, valutare la possibilità di abilitarli mediante gli insiemi di autorizzazioni. Per ulteriori informazioni, vedere Insiemi di autorizzazioni.

1. Da Imposta, immettere `Profili` nella casella `Ricerca veloce`, quindi selezionare **Profili**.
2. Nella pagina di elenco dei profili, eseguire una delle seguenti operazioni:
   - Fare clic su **Nuovo profilo** e selezionare un profilo esistente simile a quello che si desidera creare.
   - Se sono abilitate le visualizzazioni elenco di profili ottimizzate, fare clic su **Clona** accanto a un profilo simile a quello che si desidera creare.
   - Fare clic sul nome di un profilo simile a quello che si desidera creare e quindi selezionare **Clona** nella pagina del profilo.

   Un nuovo profilo utilizza la stessa licenza utente del profilo da cui è stato clonato.
3. Immettere un nome per il profilo.
4. Fare clic su **Salva**.

VEDERE ANCHE:

Profili

## Visualizzazione degli utenti assegnati a un profilo

Per visualizzare tutti gli utenti assegnati a un profilo dalla pagina della panoramica dei profili, fare clic su **Utenti assegnati** (nell'interfaccia utente profilo ottimizzata) o su **Visualizza utenti** (nell'interfaccia utente profilo originale). Dalla pagina Utenti assegnati è possibile:

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

- Creare uno o più utenti
- Reimpostare le password per gli utenti selezionati
- Modificare un utente
- Visualizzare la pagina dei dettagli di un utente facendo clic sul nome, sull'alias o sul nome utente
- Visualizzare o modificare un profilo facendo clic sul nome del profilo
- Se nell'organizzazione è abilitata Google Apps™, esportare gli utenti in Google e creare account di Google Appsfacendo clic su **Esporta in Google Apps**

VEDERE ANCHE:

Profili

## Modifica delle autorizzazioni oggetto nei profili

Le autorizzazioni oggetto specificano il tipo di accesso agli oggetti di cui dispongono gli utenti.

1. Da Imposta:
   - Immettere *Insiemi di autorizzazioni* nella casella Ricerca veloce, quindi selezionare **Insiemi di autorizzazioni** oppure
   - Immettere *Profili* nella casella Ricerca veloce, quindi selezionare **Profili**
2. Selezionare un insieme di autorizzazioni o un profilo.
3. A seconda dell'interfaccia utilizzata, eseguire una delle seguenti operazioni:
   - Insiemi di autorizzazioni o interfaccia utente profilo ottimizzata: nella casella **Trova impostazioni...**, digitare il nome dell'oggetto e selezionarlo dall'elenco. Fare clic su **Modifica**, quindi far scorrere l'elenco fino alla sezione Autorizzazioni oggetto.
   - Interfaccia utente profilo originale: fare clic su **Modifica**, quindi far scorrere l'elenco fino alla sezione Autorizzazioni oggetto standard, Autorizzazioni oggetto personalizzato o Autorizzazioni oggetto esterno.
4. Specificare le autorizzazioni oggetto.
5. Fare clic su **Salva**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le autorizzazioni oggetto:
- "Visualizza impostazione e configurazione"

Per modificare le autorizzazioni oggetto:
- "Gestisci profili e insiemi di autorizzazioni"

  E

  "Personalizza applicazione"

VEDERE ANCHE:

Autorizzazioni sugli oggetti

Profili

## Visualizzazione e modifica delle impostazioni delle schede negli insiemi di autorizzazioni e nei profili

Le impostazioni delle schede specificano se una scheda appare nella pagina Tutte le schede o è visibile in un gruppo di schede.

1. Da Imposta:
   - Immettere `Insiemi di autorizzazioni` nella casella `Ricerca veloce`, quindi selezionare **Insiemi di autorizzazioni** oppure
   - Immettere `Profili` nella casella `Ricerca veloce`, quindi selezionare **Profili**
2. Selezionare un insieme di autorizzazioni o un profilo.
3. Eseguire una delle seguenti operazioni:
   - Insiemi di autorizzazioni o interfaccia utente profilo ottimizzata: nella casella **Trova impostazioni...**, immettere il nome della scheda desiderata e selezionarla dall'elenco, quindi fare clic su **Modifica**.
   - Interfaccia utente profilo originale: fare clic su **Modifica**, quindi far scorrere l'elenco fino alla sezione Impostazioni schede.
4. Specificare le impostazioni della scheda.
5. (Solo interfaccia utente profilo originale) Per riportare le personalizzazioni delle schede di un utente all'impostazione di visibilità desiderata, selezionare **Sovrascrivi personalizzazioni schede personali degli utenti**.
6. Fare clic su **Salva**.

Nota: Se Salesforce CRM Content è abilitato per l'organizzazione ma la casella di controllo **Utente Salesforce CRM Content** non è selezionata nella pagina dei dettagli dell'utente, l'applicazione Salesforce CRM Content non avrà schede.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni delle schede:
- "Visualizza impostazione e configurazione"

Per modificare le impostazioni delle schede:
- "Gestisci profili e insiemi di autorizzazioni"

VEDERE ANCHE:

Profili

### Impostazioni delle schede

Le impostazioni delle schede specificano se una scheda appare nella pagina Tutte le schede oppure è visibile nella relativa applicazione associata. Le etichette delle impostazioni delle schede negli insiemi di autorizzazioni sono diverse dalle etichette nei profili.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in tutte le versioni tranne **Database.com**

| Impostazioni abilitate negli insiemi di autorizzazioni | Impostazioni abilitate nei profili | Descrizione |
|---|---|---|
| `Disponibile` | `Impostazioni predefinite disattivate` | La scheda è disponibile nella pagina Tutte le schede. I singoli utenti possono personalizzare la propria visualizzazione per rendere la scheda visibile in qualsiasi applicazione. |

| Impostazioni abilitate negli insiemi di autorizzazioni | Impostazioni abilitate nei profili | Descrizione |
| --- | --- | --- |
| `Disponibile` e `Visibile` | `Impostazioni predefinite attivate` | La scheda è disponibile nella pagina Tutte le schede e appare nelle schede visibili dell'applicazione associata. I singoli utenti possono personalizzare la propria visualizzazione per nascondere o rendere la scheda visibile in altre applicazioni. |
| Nessuno | `Scheda nascosta` | La scheda non è disponibile nella pagina Tutte le schede né visibile in alcuna applicazione. |

Nota: Se un utente ha un altro insieme di autorizzazioni o un profilo con impostazioni abilitate per la stessa scheda, si applicheranno le impostazioni più permissive. Si supponga ad esempio che l'insieme di autorizzazioni A non disponga di impostazioni abilitate per la scheda Account e che l'insieme di autorizzazioni B abilita l'impostazione `Disponibile` per la scheda Account. Se gli insiemi di autorizzazioni A e B vengono assegnati a un utente, l'utente vedrà la scheda Account nella pagina Tutte le schede.

VEDERE ANCHE:

Visualizzazione e modifica delle impostazioni delle schede negli insiemi di autorizzazioni e nei profili

## Panoramica sull'interfaccia utente profilo ottimizzata

L'interfaccia utente profilo ottimizzata razionalizza la gestione dei profili. Essa facilita la navigazione e la ricerca all'interno di un profilo, oltre alla modifica delle relative impostazioni.

Per abilitare l'interfaccia utente profilo ottimizzata, da Imposta immettere *`Interfaccia utente`* nella casella `Ricerca veloce`, selezionare **Interfaccia utente**, quindi selezionare **Abilita interfaccia utente profilo ottimizzata** e fare clic su **Salva**. L'organizzazione può utilizzare una sola interfaccia utente profilo alla volta.

Nota: Non è possibile utilizzare l'interfaccia utente profilo ottimizzata se:

- Per gestire i profili si utilizza Microsoft® Internet Explorer® 6 o una versione precedente (a meno di non avere installato il plug-in di Google Chrome Frame™ per Internet Explorer).
- L'organizzazione adotta i gruppi di categorie sui profili guest utilizzati per i siti.
- L'organizzazione delega l'amministrazione del portale partner agli utenti del portale.

VEDERE ANCHE:

Uso della pagina Panoramica sui profili nell'interfaccia utente profilo ottimizzata

Profili

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per abilitare l'interfaccia utente profilo ottimizzata:

- "Personalizza applicazione"

## Uso della pagina Panoramica sui profili nell'interfaccia utente profilo ottimizzata

Nell'interfaccia utente profilo ottimizzata, la pagina con la panoramica dei profili consente di specificare tutte le impostazioni e le autorizzazioni di un profilo.

Per aprire la pagina con la panoramica dei profili, da Imposta immettere `Profili` nella casella `Ricerca veloce`, quindi selezionare **Profili** e fare clic sul profilo da visualizzare.

Dalla pagina Panoramica sui profili è possibile:

- Cercare un oggetto, un'autorizzazione o un'impostazione
- Clonare il profilo
- Se si tratta di un profilo personalizzato, eliminarlo facendo clic su **Elimina**

  Nota: non è possibile eliminare un profilo assegnato a un utente, anche se l'utente è inattivo.

- Modificare il nome o la descrizione del profilo facendo clic su **Modifica proprietà**
- Visualizzare un elenco degli utenti assegnati al profilo
- In Applicazioni e Sistema, fare clic su uno dei link per visualizzare o modificare autorizzazioni e impostazioni.

VEDERE ANCHE:

Panoramica sull'interfaccia utente profilo ottimizzata

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare i profili:
- "Visualizza impostazione e configurazione"

Per eliminare i profili e modificarne le proprietà:
- "Gestisci profili e insiemi di autorizzazioni"

## Impostazioni delle applicazioni e di sistema nell'interfaccia utente profilo ottimizzata

Nell'interfaccia utente profilo ottimizzata, gli amministratori possono agevolmente navigare e cercare fra le impostazioni di un singolo profilo, nonché modificarle. Autorizzazioni e impostazioni sono suddivise in pagine classificate come applicazioni e sistema, che rispecchiano le autorizzazioni richieste agli utenti per amministrare e utilizzare le applicazioni e le risorse del sistema.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

### Impostazioni applicazione

Le applicazioni sono gruppi di schede che gli utenti possono modificare selezionando il menu a discesa nell'intestazione. Tutti gli oggetti, i componenti, i dati e le configurazioni sottostanti restano invariati, indipendentemente dall'applicazione selezionata. Con la selezione di un'applicazione, gli utenti si spostano in un gruppo di schede che consentono di utilizzare in modo efficiente le funzionalità sottostanti per le operazioni specifiche di un'applicazione. Si immagini ad esempio di svolgere la maggior parte del proprio lavoro nell'applicazione di vendita, che contiene schede come Account e Opportunità. Per monitorare una nuova campagna di marketing, anziché aggiungere la scheda Campagne all'applicazione di vendita è possibile selezionare Marketing dal menu a discesa delle applicazioni per visualizzare le proprie campagne e i relativi membri.

Nell'interfaccia utente profilo ottimizzata, la sezione Applicazioni della pagina introduttiva contiene le impostazioni direttamente associate ai processi aziendali resi possibili dalle applicazioni. Ad esempio, gli agenti dell'assistenza clienti potrebbero avere necessità di gestire i casi, per cui l'autorizzazione "Gestisci casi" si trova nella sezione Call Center della pagina Autorizzazioni applicazione. Alcune impostazioni delle applicazioni non sono correlate alle autorizzazioni applicazione. Ad esempio, per abilitare l'applicazione di gestione dei permessi da AppExchange, gli utenti devono poter accedere alle classi Apex e alle pagine Visualforce appropriate, nonché disporre delle autorizzazioni oggetti e campi che consentono di creare nuove richieste di permessi.

**Nota:** le autorizzazioni degli utenti vengono rispettate integralmente, a prescindere dall'applicazione selezionata. Ad esempio, benché l'autorizzazione "Importa lead" si trovi nella categoria Vendite, gli utenti possono importare i lead anche quando si trovano nell'applicazione Call Center.

### Impostazioni di sistema

Alcune funzioni del sistema sono valide per l'organizzazione anziché per una singola applicazione. Ad esempio, gli orari di accesso e gli intervalli IP di accesso controllano la possibilità di accesso dell'utente, indipendentemente dall'applicazione a cui questi accede. Altre funzioni del sistema sono valide per tutte le applicazioni. Ad esempio, le autorizzazioni "Esegui rapporti" e "Gestisci cruscotti digitali" permettono ai responsabili di creare e gestire rapporti in tutte le applicazioni. In alcuni casi, ad esempio con "Modifica tutti i dati", un'autorizzazione è valida per tutte le applicazioni ma comprende anche funzioni che esulano da queste ultime come la possibilità di scaricare Data Loader.

VEDERE ANCHE:

Panoramica sull'interfaccia utente profilo ottimizzata

## Ricerca nell'interfaccia utente profilo ottimizzata

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Le autorizzazioni e le impostazioni disponibili per i profili variano a seconda della versione di Salesforce utilizzata.

AUTORIZZAZIONI UTENTE

Per cercare autorizzazioni e impostazioni in un profilo:
- "Visualizza impostazione e configurazione"

Per individuare il nome di un oggetto, di una scheda, di un'autorizzazione o di un'impostazione su una pagina del profilo, digitare almeno tre lettere consecutive nella casella **Trova impostazioni**. Via via che si digitano i caratteri, vengono elencati i suggerimenti relativi ai risultati corrispondenti ai termini di ricerca inseriti. Fare clic su una voce dell'elenco per accedere alla relativa pagina delle impostazioni.

I termini della ricerca non fanno distinzione tra caratteri maiuscoli e minuscoli. Per alcune categorie, è possibile cercare il nome dell'autorizzazione o dell'impostazione specifica. Per le altre categorie, eseguire la ricerca per nome di categoria.

| Voce | Ricerca di | Esempio |
|---|---|---|
| Applicazioni assegnate | Nome applicazione | Digitare `vendite` nella casella Trova impostazioni e selezionare `Vendite` dall'elenco. |
| Oggetti | Nome oggetto | Si supponga di avere un oggetto personalizzato denominato Album. Digitare `albu`, quindi selezionare `Album`. |
| • Campi<br>• Tipi di record<br>• Assegnazioni al layout di pagina | Nome oggetto principale | Si supponga che l'oggetto Album contenga un campo Descrizione. Per trovare il campo `Descrizione` tra gli album, digitare `albu`, selezionare `Album` e scorrere verso il basso fino a `Descrizione` in Autorizzazioni campi. |
| Schede | Nome scheda o oggetto principale | Digitare `rap` e quindi selezionare `Rapporti`. |
| Autorizzazioni di applicazioni e sistema | Nome autorizzazione | Digitare `api` e selezionare `API abilitata`. |

| Voce | Ricerca di | Esempio |
| --- | --- | --- |
| Tutte le altre categorie | Nome categoria | Per trovare le impostazioni di accesso della classe Apex, digitare *apex*, quindi selezionare `Accesso classe Apex`. Per trovare le autorizzazioni personalizzate, digitare *pers*, quindi selezionare `Autorizzazioni personalizzate`. E così via. |

Se nella ricerca non appaiono risultati:

- Verificare che l'autorizzazione, l'oggetto, la scheda o l'impostazione oggetto della ricerca sia disponibile nell'organizzazione corrente.
- Verificare che la voce oggetto della ricerca sia disponibile per la licenza utente associata al profilo corrente. Ad esempio, un profilo con licenza Portale Clienti a volume elevato non include l'autorizzazione "Modifica tutti i dati".
- Controllare che i termini di ricerca includano almeno tre caratteri consecutivi dell'elemento che si desidera ricercare.
- Assicurarsi che l'ortografia del termine cercato sia corretta.

VEDERE ANCHE:

Panoramica sull'interfaccia utente profilo ottimizzata

## Assegnazione dei tipi di record e dei layout di pagina nell'interfaccia utente profilo ottimizzata

Nell'interfaccia utente profilo ottimizzata, le impostazioni dei tipi di record e delle assegnazioni dei layout di pagina determinano la mappatura dei tipi di record e dell'assegnazione dei layout di pagina utilizzata quando gli utenti visualizzano i record. Determinano inoltre i tipi di record disponibili quando gli utenti creano o modificano record.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni di accesso ai layout di pagina e ai tipi di record:

- "Gestisci profili e insiemi di autorizzazioni"

Per specificare i tipi di record e le assegnazioni dei layout di pagina:

1. Da Imposta, immettere *Profili* nella casella `Ricerca veloce`, quindi selezionare **Profili**.
2. Selezionare un profilo.
3. Nella casella **Trova impostazioni...**, digitare il nome dell'oggetto desiderato e selezionarlo dall'elenco.
4. Fare clic su **Modifica**.
5. Nella sezione Tipi di record e assegnazioni layout di pagina, modificare le impostazioni in funzione delle proprie esigenze.

| Impostazione | Descrizione |
| --- | --- |
| Tipi di record | Elenca tutti i tipi di record esistenti per l'oggetto.<br>`--Principale--` è un tipo di record generato dal sistema utilizzato quando a un record non è associato un tipo di record personalizzato. Quando si assegna il tipo di record `--Principale--`, gli utenti non possono impostare il tipo di un record (ad esempio durante la creazione del record). Tutti gli altri tipi di record sono tipi di record personalizzati. |

| Impostazione | Descrizione |
| --- | --- |
| Assegnazione layout di pagina | Il layout di pagina da utilizzare per ogni tipo di record. Il layout di pagina determina i pulsanti, i campi, gli elenchi correlati e gli altri elementi visualizzati dagli utenti con quel profilo durante la creazione di record con il tipo di record associato. Poiché tutti gli utenti possono accedere a tutti i tipi di record, a ogni tipo di record deve essere assegnato un layout di pagina, anche se il tipo di record non è specificato come tipo di record assegnato nel profilo. |
| Tipi di record assegnati | I tipi di record selezionati in questa colonna sono disponibili quando gli utenti con questo profilo creano record per l'oggetto. Se si seleziona `--Principale--` non è possibile selezionare alcun tipo di record personalizzato, e se si selezionano tipi di record personalizzati non è possibile selezionare `--Principale--`. |
| Tipo di record predefinito | Il tipo di record predefinito da utilizzare quando gli utenti con questo profilo creano record per l'oggetto. |

Le impostazioni Tipi di record e assegnazioni layout di pagina presentano alcune varianti per gli oggetti e le schede che seguono.

| Oggetto o scheda | Variante |
| --- | --- |
| Account | Se l'organizzazione utilizza gli account personali, l'oggetto account include anche le impostazioni per il **tipo di record predefinito account aziendale** e per il **tipo di record predefinito account personale**, che indicano il tipo di record predefinito da utilizzare quando gli utenti con quel profilo creano record account aziendali o personali da lead convertiti. |
| Casi | L'oggetto casi include anche le impostazioni **Chiusura dei casi**, che mostrano le assegnazioni dei layout di pagina da utilizzare per ogni tipo di record nei casi chiusi. Questo significa che il medesimo tipo di record può avere layout di pagina diversi per i casi aperti e per quelli chiusi. Con questa impostazione aggiuntiva, quando gli utenti chiudono un caso questo può avere un layout di pagina diverso che indica come è stato chiuso. |
| Pagina iniziale | Non è possibile specificare tipi di record personalizzati per la scheda Pagina iniziale. È possibile solo selezionare un'assegnazione layout di pagina per il tipo di record --Principale--. |

6. Fare clic su **Salva**.

VEDERE ANCHE:

Come viene specificato l'accesso ai tipi di record?

Assegnazione di tipi di record personalizzati negli insiemi di autorizzazioni

Uso della pagina Panoramica sui profili nell'interfaccia utente profilo ottimizzata

## Visualizzazione e modifica degli orari di accesso nell'interfaccia utente profilo ottimizzata

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni degli orari di accesso:

- "Visualizza impostazione e configurazione"

Per modificare le impostazioni degli orari di accesso:

- "Gestisci profili e insiemi di autorizzazioni"

Per ogni profilo è possibile specificare gli orari in cui gli utenti possono effettuare l'accesso.

1. Da Imposta, immettere `Profili` nella casella `Ricerca veloce`, quindi selezionare **Profili**.
2. Selezionare un profilo e fare clic sul nome corrispondente.
3. Nella pagina con la panoramica dei profili, scorrere fino a Orari di accesso e fare clic su **Modifica**.
4. Impostare i giorni e gli orari nei quali gli utenti con quel profilo possono accedere all'organizzazione.

   Per consentire agli utenti di eseguire l'accesso in qualsiasi orario, fare clic su **Cancella tutti gli orari**. Per impedire agli utenti l'utilizzo del sistema durante un giorno specifico, impostare gli orari di inizio e termine sullo stesso valore.

   Gli utenti ancora collegati al termine del loro orario di accesso possono continuare a visualizzare la pagina corrente ma non possono eseguire ulteriori operazioni.

Nota: la prima volta che si impostano per un profilo, gli orari di accesso si basano sul `Fuso orario predefinito` dell'organizzazione specificato in Imposta, nella pagina Informazioni sulla società. Dopo tale impostazione, eventuali modifiche apportate al `Fuso orario predefinito` dell'organizzazione non determineranno la modifica del fuso orario per gli orari di accesso del profilo. Di conseguenza, gli orari di accesso vengono applicati sempre a quegli intervalli esatti, anche se un utente si trova in un fuso orario diverso o se viene modificato il fuso orario predefinito dell'organizzazione.

Gli orari possono apparire in modo diverso a seconda che si stiano visualizzando o modificando gli orari di accesso. Nella pagina di modifica Orari di accesso, gli orari sono visualizzati nel fuso orario specificato. Nella pagina con la panoramica dei profili sono visualizzati nel fuso orario originale dell'organizzazione.

VEDERE ANCHE:

Panoramica sull'interfaccia utente profilo ottimizzata

## Limitazione degli intervalli IP di accesso nell'interfaccia utente profilo ottimizzata

È possibile controllare l'accesso in un profilo utente specificando un intervallo di indirizzi IP. Quando si definiscono le limitazioni degli indirizzi IP per un profilo, viene negato ogni tipo di accesso dall'indirizzo IP limitato.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare gli intervalli IP di accesso:
- "Visualizza impostazione e configurazione"

Per modificare ed eliminare gli intervalli IP di accesso:
- "Gestisci profili e insiemi di autorizzazioni"

1. Da Imposta, immettere *Profili* nella casella `Ricerca veloce`, quindi selezionare **Profili**.
2. Selezionare un profilo e fare clic sul nome corrispondente.
3. Nella pagina della panoramica dei profili, fare clic su **Intervalli IP di accesso**.
4. Per modificare gli intervalli di indirizzi IP di accesso per il profilo, utilizzare uno dei metodi descritti di seguito.
   - Per aggiungere intervalli, fare clic su **Aggiungi intervalli IP**. Immettere un indirizzo IP valido nel campo `Indirizzo IP iniziale` e un indirizzo IP superiore nel campo `Indirizzo IP finale`. Gli indirizzi iniziale e finale definiscono l'intervallo degli indirizzi IP consentiti da cui gli utenti possono eseguire l'accesso. Per consentire gli accessi da un unico indirizzo IP, immettere lo stesso indirizzo nei due campi. Ad esempio, per consentire l'accesso solo da 125.12.3.0, digitare 125.12.3.0 sia come indirizzo iniziale che come indirizzo finale.
   - Per modificare o rimuovere gli intervalli, fare clic su **Modifica** o **Elimina** per il singolo intervallo.
   - Se lo si desidera, immettere una descrizione per l'intervallo. Se si tengono più intervalli, utilizzare il campo Descrizione per indicare i dettagli, ad esempio a quale parte della rete corrisponde un determinato intervallo.

   Entrambi gli indirizzi IP in un intervallo devono essere IPv4 o IPv6. Negli intervalli, gli indirizzi IPv4 esistono nello spazio degli indirizzi IPv6 mappati a IPv4 da `::ffff:0:0` a `::ffff:ffff:ffff`, dove `::ffff:0:0` è `0.0.0.0` e `::ffff:ffff:ffff` è `255.255.255.255`. Un intervallo non può includere indirizzi IP all'interno dello spazio degli indirizzi IPv6 mappati a IPv4 se contiene anche indirizzi IP esterni allo spazio degli indirizzi IPv6 mappati a IPv4. Intervalli come da `255.255.255.255` a `::1:0:0:0` o da `::` a `::1:0:0:0` non sono consentiti. È possibile impostare indirizzi IPv6 in tutte le organizzazioni, ma a partire dal rilascio Spring '12 IPv6 è abilitato solo per l'accesso alle organizzazioni Sandbox.

   Importante:

   - Per i profili Utente partner gli indirizzi IP sono limitati a 5. Per incrementare questo limite, contattare Salesforce.
   - L'applicazione Salesforce Classic mobile può aggirare le definizioni dell'intervallo IP impostate per i profili. Salesforce Classic mobile stabilisce una connessione protetta a Salesforce sulla rete dell'operatore mobile, i cui indirizzi IP potrebbero tuttavia trovarsi al di fuori degli intervalli IP consentiti per il profilo dell'utente. Per evitare che le definizioni degli indirizzi IP impostate sul profilo di un utente vengano aggirate, disabilitare Salesforce Classic mobile a pagina 713 per quell'utente.

Nota: è possibile limitare l'accesso a Salesforce esclusivamente agli indirizzi IP compresi negli Intervalli IP di accesso. Si supponga ad esempio che un utente esegua correttamente l'accesso da un indirizzo IP definito negli Intervalli IP di accesso. In seguito, l'utente si sposta in un punto diverso e gli viene assegnato un nuovo indirizzo IP, che non rientra negli Intervalli IP di accesso. Quando l'utente tenta di accedere a Salesforce, anche da un'applicazione client, l'accesso gli viene negato. Per abilitare questa opzione, da Imposta immettere *Impostazioni di sessione* nella casella `Ricerca veloce`, selezionare **Impostazioni di sessione**, quindi selezionare **Imponi intervalli IP di accesso su ogni richiesta**. Questa opzione riguarda tutti i profili utente con restrizioni IP di accesso.

## Uso dei profili nell'interfaccia profilo originale

Per visualizzare un profilo, da Imposta immettere *Profili* nella casella `Ricerca veloce`, quindi selezionare **Profili** e selezionare il profilo desiderato.

Nella pagina dei dettagli del profilo è possibile:

- Modificare il profilo
- Creare un profilo basato su quel profilo
- Solo nel caso dei profili personalizzati, è possibile fare clic su **Elimina** per eliminare un profilo.

  Nota: non è possibile eliminare un profilo assegnato a un utente, anche se l'utente è inattivo.

- Visualizzare gli utenti assegnati a quel profilo

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

## Modifica dei profili nell'interfaccia profilo originale

I profili definiscono il modo in cui gli utenti accedono a oggetti e dati e cosa possono fare all'interno dell'applicazione. Nei profili standard, è possibile modificare una serie limitata di impostazioni. Nei profili personalizzati, è possibile modificare tutte le autorizzazioni e le impostazioni disponibili ad eccezione della licenza utente.

Nota: la modifica di alcune autorizzazioni può comportare l'abilitazione o la disabilitazione di altre autorizzazioni. Ad esempio, se si abilita l'autorizzazione "Visualizza tutti i dati" viene abilitata l'autorizzazione "Lettura" per tutti gli oggetti. Analogamente, l'autorizzazione "Trasferisci lead" abilita le autorizzazioni "Lettura" e "Crea" sui lead.

Suggerimento: Se nell'organizzazione sono abilitate le visualizzazioni elenco profili ottimizzate, è possibile cambiare le autorizzazioni di più profili dalla visualizzazione elenco.

1. Da Imposta, immettere *Profili* nella casella `Ricerca veloce`, quindi selezionare **Profili**.
2. Selezionare il profilo che si desidera modificare.
3. Nella pagina dei dettagli del profilo, fare clic su **Modifica**.

VEDERE ANCHE:

Assegnazione dei layout di pagina nell'interfaccia utente profilo originale

Impostazioni del profilo nell'interfaccia profilo originale

Visualizzazione e modifica dell'accesso ai client desktop nell'interfaccia utente profilo originale

Assegnazione di tipi di record ai profili nell'interfaccia utente profilo originale

Visualizzazione e modifica degli orari di accesso nell'interfaccia utente profilo originale

Limitazione degli indirizzi IP di accesso nell'interfaccia utente profilo originale

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per modificare i profili:
- "Gestisci profili e insiemi di autorizzazioni"

  E

  "Personalizza applicazione"

## Impostazioni del profilo nell'interfaccia profilo originale

I profili definiscono il modo in cui gli utenti accedono a oggetti e dati e cosa possono fare all'interno dell'applicazione. Visualizzare o modificare queste impostazioni dalla pagina dei dettagli del profilo originale.

| Impostazione | Per visualizzare o modificare, accedere a |
| --- | --- |
| Nome e descrizione del profilo (solo profili personalizzati) | Dettagli del profilo |
| Autorizzazioni amministrative e generali (solo profili personalizzati) | Autorizzazioni amministrative |
| Impostazioni di visibilità delle applicazioni | Impostazioni delle applicazioni personalizzate |
| Layout di console per tutti i profili | Impostazioni console |
| Autorizzazioni personalizzate | Autorizzazioni personalizzate abilitate |
| Impostazioni di accesso client desktop | Client di integrazione desktop |
| Fonti di dati esterne | Accesso fonte di dati esterna abilitato |
| Accesso ai campi negli oggetti | Protezione livello campo |
| Orari di accesso | Orari di accesso |
| Intervalli di indirizzi IP di accesso | Nella sezione Intervalli IP di accesso, fare clic su **Nuovo** oppure fare clic su **Modifica** accanto a un intervallo IP esistente.<br><br>Nota: è possibile limitare l'accesso a Salesforce esclusivamente agli indirizzi IP compresi negli Intervalli IP di accesso. Si supponga ad esempio che un utente esegua correttamente l'accesso da un indirizzo IP definito negli Intervalli IP di accesso. In seguito, l'utente si sposta in un punto diverso e gli viene assegnato un nuovo indirizzo IP, che non rientra negli Intervalli IP di accesso. Quando l'utente tenta di accedere a Salesforce, anche da un'applicazione client, l'accesso gli viene negato. Per abilitare questa opzione, da Imposta immettere *`Impostazioni di sessione`* nella casella `Ricerca veloce`, selezionare **Impostazioni di sessione**, quindi selezionare **Imponi intervalli IP di accesso su ogni richiesta**. Questa opzione riguarda tutti i profili utente con restrizioni IP di accesso. |

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per modificare i profili:
- "Gestisci profili e insiemi di autorizzazioni"

  E

  "Personalizza applicazione"

| Impostazione | Per visualizzare o modificare, accedere a |
|---|---|
| Autorizzazioni oggetto | Autorizzazioni oggetti standard |
| Layout di pagina | Layout di pagina |
| Tipi di record | Sezione Impostazioni tipo di record. Il link **Modifica** è visualizzato solo se per l'oggetto esistono dei tipi di record. |
| Impostazioni di visibilità delle schede | Impostazioni delle schede |
| Classi Apex eseguibili | Accesso classe Apex abilitato |
| Pagine Visualforce eseguibili | Accesso alle pagine Visualforce abilitato |
| Stati presenza dell'assistenza | Accesso stati presenza dell'assistenza abilitato |

VEDERE ANCHE:

Modifica dei profili nell'interfaccia profilo originale

## Assegnazione dei layout di pagina nell'interfaccia utente profilo originale

Se si sta già utilizzando un'interfaccia utente profilo originale, è possibile accedere agevolmente a tutte le assegnazioni dei layout di pagina, visualizzarle e modificarle da un'unica posizione.

1. Da Imposta, immettere `Profili` nella casella `Ricerca veloce`, quindi selezionare **Profili**.
2. Selezionare un profilo.
3. Fare clic su **Visualizza assegnazione** accanto al nome di una scheda nella sezione Layout di pagina.
4. Fare clic su **Modifica assegnazione**.
5. Utilizzare la tabella per specificare il layout di pagina appropriato per ciascun profilo. Se l'organizzazione utilizza tipi di record, una matrice visualizza un selettore layout di pagina per ogni profilo e tipo di record.
   - Le assegnazioni dei layout di pagina selezionate sono evidenziate.
   - Le assegnazioni dei layout di pagina in corso di modifica sono visualizzate in corsivo finché non si salvano le modifiche.
6. Se necessario, selezionare un altro layout di pagina dall'elenco a discesa `Layout di pagina da utilizzare` e ripetere le operazioni precedenti per il nuovo layout di pagina.
7. Fare clic su **Salva**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per assegnare layout di pagina nei profili:
- "Gestisci profili e insiemi di autorizzazioni"

VEDERE ANCHE:

Uso dei profili nell'interfaccia profilo originale

## Visualizzazione e modifica dell'accesso ai client desktop nell'interfaccia utente profilo originale

Connect Offline e Connect per Office sono client desktop che consentono di integrare Salesforce nel PC in uso. In qualità di amministratore, è possibile controllare quali client desktop sono accessibili agli utenti, nonché decidere se inviare automaticamente una notifica agli utenti non appena sono disponibili eventuali aggiornamenti.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni di accesso ai client desktop:
- "Visualizza impostazione e configurazione"

Per modificare le impostazioni di accesso ai client desktop:
- "Gestisci profili e insiemi di autorizzazioni"

Nota: Per accedere ai client desktop, gli utenti devono inoltre disporre dell'autorizzazione "API abilitata".

1. Da Imposta, immettere *Profili* nella casella `Ricerca veloce`, quindi selezionare **Profili**.
2. Fare clic su **Modifica** accanto al nome di un profilo e scorrere fino alla sezione Client integrazione desktop nella parte inferiore della pagina.

VEDERE ANCHE:

Uso dei profili nell'interfaccia profilo originale

## Assegnazione di tipi di record ai profili nell'interfaccia utente profilo originale

Dopo aver creato i tipi di record e incluso in essi i valori degli elenchi di selezione, aggiungere i tipi di record ai profili utente. Se si assegna un tipo di record a un profilo, gli utenti con il profilo specificato possono assegnare quel tipo di record ai record creati o modificati.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per assegnare tipi di record ai profili:
- "Personalizza applicazione"

Nota: Gli utenti possono visualizzare record di qualsiasi tipo, anche se il tipo di record non è associato al loro profilo.

È possibile associare diversi tipi di record a un profilo. Si supponga ad esempio che un utente debba creare delle opportunità di vendita per hardware e software. In questo caso, è possibile creare e aggiungere entrambi i tipi di record "Hardware" e "Software" al profilo dell'utente.

1. Da Imposta, immettere *Profili* nella casella `Ricerca veloce`, quindi selezionare **Profili**.
2. Selezionare un profilo. I tipi di record disponibili per quel profilo sono elencati nella sezione Impostazioni tipo di record.
3. Fare clic su **Modifica** accanto al tipo adeguato di record.
4. Selezionare un tipo di record dall'elenco Tipi di record disponibili e aggiungerlo all'elenco Tipi di record selezionati.

   **Principale** è un tipo di record generato dal sistema, utilizzato quando a un determinato record non è associato alcun tipo di record personalizzato. Quando si assegna il tipo di record `Principale`, gli utenti non possono impostare il tipo di un record (ad esempio durante la creazione del record). Tutti gli altri tipi di record sono personalizzati.

5. Da `Predefinito`, scegliere un tipo di record predefinito.

   Se l'organizzazione utilizza account personali, questa impostazione controlla anche i campi account che vengono visualizzati nella sezione `Creazione rapida` della pagina iniziale Account.

6. Se l'organizzazione utilizza account personali, impostare le opzioni per i tipi di record predefiniti sia per gli account personali, sia per gli account aziendali. Scegliere un tipo di record predefinito dall'elenco a discesa `Tipo di record predefinito account aziendale` e `Tipo di record predefinito account personale`.

   Queste impostazioni vengono utilizzate quando sono necessari valori predefiniti per entrambi i tipi di account, ad esempio durante la conversione di lead.

7. Fare clic su **Salva**.

Nota: se l'organizzazione utilizza account personali, è possibile visualizzare i tipi di record predefiniti sia per gli account personali, sia per gli account aziendali. Accedere a Impostazioni tipo di record degli account nella pagina dei dettagli del profilo. Per iniziare a impostare i tipi di record predefiniti per gli account è anche possibile fare clic su **Modifica** in Impostazioni tipo di record degli account.

VEDERE ANCHE:

Come viene specificato l'accesso ai tipi di record?

Uso dei profili nell'interfaccia profilo originale

Assegnazione di tipi di record personalizzati negli insiemi di autorizzazioni

## Visualizzazione e modifica degli orari di accesso nell'interfaccia utente profilo originale

Specificare gli orari in cui gli utenti possono eseguire l'accesso in base al profilo utente.

1. Da Imposta, immettere *`Profili`* nella casella `Ricerca veloce`, quindi selezionare **Profili** e selezionare un profilo.
2. Fare clic su **Modifica** nell'elenco correlato Orari di accesso.
3. Impostare i giorni e gli orari nei quali gli utenti con questo profilo possono utilizzare il sistema.

   Per consentire agli utenti di eseguire l'accesso in qualsiasi orario, fare clic su **cancella tutti gli orari**. Per impedire agli utenti l'utilizzo del sistema durante un giorno specifico, impostare gli orari di inizio e termine sullo stesso valore.

   Gli utenti ancora collegati al termine del loro orario di accesso possono continuare a visualizzare la pagina corrente ma non possono eseguire ulteriori operazioni.

4. Fare clic su **Salva**.

Nota: La prima volta che vengono impostati per un profilo, gli orari di accesso si basano sul `Fuso orario predefinito` dell'organizzazione specificato nella pagina Informazioni sulla società in Imposta. Dopo tale impostazione, eventuali modifiche apportate al `Fuso orario predefinito` dell'organizzazione non determineranno la modifica del fuso orario per gli orari di accesso del profilo. Di conseguenza, gli orari di accesso vengono applicati sempre a quegli intervalli esatti, anche se un utente si trova in un fuso orario diverso o se viene modificato il fuso orario predefinito dell'organizzazione.

Gli orari possono apparire in modo diverso a seconda che si stiano visualizzando o modificando gli orari di accesso. Nella pagina dei dettagli del profilo, gli orari sono visualizzati nel fuso

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per impostare l'orario di accesso:

- "Gestisci profili e insiemi di autorizzazioni"

orario specificato. Nella pagina di modifica degli orari di accesso, gli orari sono visualizzati nel fuso orario dell'organizzazione.

VEDERE ANCHE:

Uso dei profili nell'interfaccia profilo originale

Limitazione degli indirizzi IP di accesso nell'interfaccia utente profilo originale

## Limitazione degli indirizzi IP di accesso nell'interfaccia utente profilo originale

È possibile controllare l'accesso in un profilo utente specificando un intervallo di indirizzi IP. Quando si definiscono le limitazioni degli indirizzi IP per un profilo, viene negato ogni tipo di accesso dall'indirizzo IP limitato.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

AUTORIZZAZIONI UTENTE

Per visualizzare gli intervalli IP di accesso:
- "Visualizza impostazione e configurazione"

Per modificare ed eliminare gli intervalli IP di accesso:
- "Gestisci profili e insiemi di autorizzazioni"

1. La procedura utilizzata per limitare l'intervallo degli indirizzi IP validi sui profili dipende dalla versione (Edition) utilizzata.
   - Se si utilizza la versione Enterprise Edition, Unlimited Edition, Performance Edition o Developer Edition, da Imposta, immettere *`Profili`* nella casella `Ricerca veloce`, quindi selezionare **Profili** e selezionare un profilo.
   - Se si utilizza la versione Professional Edition, Group Edition o Personal Edition, da Imposta, immettere *`Impostazioni di sessione`* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di sessione**.
2. Fare clic su **Nuovo** nell'elenco correlato Intervalli IP di accesso.
3. Immettere un indirizzo IP valido nel campo `Indirizzo IP iniziale` e un indirizzo IP superiore nel campo `Indirizzo IP finale`.

   Gli indirizzi iniziale e finale definiscono l'intervallo degli indirizzi IP consentiti da cui gli utenti possono eseguire l'accesso. Per consentire gli accessi da un unico indirizzo IP, immettere lo stesso indirizzo nei due campi. Ad esempio, per consentire l'accesso solo da 125.12.3.0, digitare 125.12.3.0 sia come indirizzo iniziale che come indirizzo finale.
   - Per i profili Utente partner gli indirizzi IP sono limitati a 5. Per incrementare questo limite, contattare Salesforce.
   - L'applicazione Salesforce Classic mobile può aggirare le definizioni dell'intervallo IP impostate per i profili. Salesforce Classic mobile stabilisce una connessione protetta a Salesforce sulla rete dell'operatore mobile, i cui indirizzi IP potrebbero tuttavia trovarsi al di fuori degli intervalli IP consentiti per il profilo dell'utente. Per evitare che le definizioni degli indirizzi IP impostate sul profilo di un utente vengano aggirate, disabilitare Salesforce Classic mobile a pagina 713 per quell'utente.
4. Se lo si desidera, immettere una descrizione per l'intervallo. Se si tengono più intervalli, utilizzare il campo Descrizione per indicare i dettagli, ad esempio a quale parte della rete corrisponde un determinato intervallo.
5. Fare clic su **Salva**.

Entrambi gli indirizzi IP in un intervallo devono essere IPv4 o IPv6. Negli intervalli, gli indirizzi IPv4 esistono nello spazio degli indirizzi IPv6 mappati a IPv4 da `::ffff:0:0` a `::ffff:ffff:ffff`, dove `::ffff:0:0` è `0.0.0.0` e `::ffff:ffff:ffff` è `255.255.255.255`. Un intervallo non può includere indirizzi IP all'interno dello spazio degli indirizzi IPv6 mappati a IPv4 se contiene anche indirizzi IP esterni allo spazio degli indirizzi IPv6 mappati a IPv4. Intervalli come da `255.255.255.255` a `::1:0:0:0` o da `::` a `::1:0:0:0` non sono consentiti. È possibile impostare indirizzi IPv6 in tutte le organizzazioni, ma a partire dal rilascio Spring '12 IPv6 è abilitato solo per l'accesso alle organizzazioni Sandbox.

Nota: Le impostazioni della cache per le risorse statiche sono impostate su private quando vi si accede mediante un sito Force.com il cui profilo utente guest presenta delle restrizioni basate sull'intervallo IP o sugli orari di accesso. I siti con restrizioni del profilo

utente guest eseguono la cache delle risorse statiche solo all'interno del browser. Inoltre, se un sito in precedenza privo di limitazioni diventa limitato, potrebbero essere necessari fino a 45 giorni prima della scadenza delle risorse statiche dalla cache di Salesforce e dalle eventuali cache intermedie.

Nota: è possibile limitare l'accesso a Salesforce esclusivamente agli indirizzi IP compresi negli Intervalli IP di accesso. Si supponga ad esempio che un utente esegua correttamente l'accesso da un indirizzo IP definito negli Intervalli IP di accesso. In seguito, l'utente si sposta in un punto diverso e gli viene assegnato un nuovo indirizzo IP, che non rientra negli Intervalli IP di accesso. Quando l'utente tenta di accedere a Salesforce, anche da un'applicazione client, l'accesso gli viene negato. Per abilitare questa opzione, in Imposta, immettere *Impostazioni di sessione* nella casella `Ricerca veloce`, selezionare **Impostazioni di sessione** e quindi **Imponi intervalli IP di accesso su ogni richiesta**. Questa opzione riguarda tutti i profili con restrizioni IP di accesso.

VEDERE ANCHE:

Impostazione degli intervalli IP affidabili per l'organizzazione

Visualizzazione e modifica degli orari di accesso nell'interfaccia utente profilo originale

Uso dei profili nell'interfaccia profilo originale

## Visualizzazione e modifica delle applicazioni assegnate nei profili

Le impostazioni delle applicazioni assegnate specificano le applicazioni che gli utenti possono selezionare nel menu delle applicazioni Force.com.

Ogni profilo deve contenere almeno un'applicazione visibile, tranne i profili associati agli utenti del Portale Clienti per i quali le applicazioni non sono disponibili.

Per specificare la visibilità delle applicazioni:

1. Da Imposta, immettere *Profili* nella casella `Ricerca veloce`, quindi selezionare **Profili**.
2. Selezionare un profilo.
3. A seconda dell'interfaccia utente utilizzata, eseguire una delle seguenti operazioni:
   - Interfaccia utente profilo ottimizzata: fare clic su **Applicazioni assegnate**, quindi fare clic su **Modifica**.
   - Interfaccia utente profilo originale: fare clic su **Modifica**, quindi scorrere fino alla sezione Impostazioni applicazioni personalizzate.
4. Selezionare un'applicazione predefinita. Quando un utente effettua il primo accesso, viene visualizzata l'applicazione predefinita.
5. Selezionare **Visibile** per qualsiasi altra applicazione che si desidera rendere visibile.

VEDERE ANCHE:

Profili

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni di visualizzazione delle applicazioni:

- "Gestisci profili e insiemi di autorizzazioni"

## Abilitazione di autorizzazioni personalizzate nei profili

Le autorizzazioni personalizzate rappresentano un modo per consentire l'accesso a processi o applicazioni personalizzate. Dopo avere creato un'autorizzazione personalizzata e averla associata a un processo o a un'applicazione, è possibile abilitarla nei profili.

1. Da Imposta, immettere `Profili` nella casella `Ricerca veloce`, quindi selezionare **Profili**.
2. Selezionare un profilo.
3. A seconda dell'interfaccia utente utilizzata, eseguire una delle seguenti operazioni:
   - Interfaccia utente profilo ottimizzata: fare clic su **Autorizzazioni personalizzate** e quindi su **Modifica**.
   - Interfaccia utente profilo originale: nell'elenco correlato Autorizzazioni personalizzate abilitate, fare clic su **Modifica**.
4. Per abilitare le autorizzazioni personalizzate, selezionarle dall'elenco Autorizzazioni personalizzate disponibili e fare clic su **Aggiungi**. Per rimuovere le autorizzazioni personalizzate dal profilo, selezionarle dall'elenco Autorizzazioni personalizzate abilitate e fare clic su **Rimuovi**.
5. Fare clic su **Salva**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Nelle organizzazioni Group Edition e Professional Edition non è possibile creare o modificare autorizzazioni personalizzate, ma è possibile installarle come parte di un pacchetto gestito.

AUTORIZZAZIONI UTENTE

Per abilitare le autorizzazioni personalizzate nei profili:

- "Gestisci profili e insiemi di autorizzazioni"

## Visualizzazione e modifica del valore di timeout delle sessioni nei profili

Utilizzare il Timeout sessione per impostare un limite alla durata della sessione di autenticazione di un utente. Al termine della sessione, l'utente dovrà effettuare nuovamente l'accesso.

Fino a quando non si imposta il Timeout sessione in un profilo, per gli utenti di quel profilo vale il `Valore timeout` dell'organizzazione definito nelle Impostazioni di sessione. Una volta configurato, il Timeout sessione di un profilo ha la precedenza sul `Valore timeout` dell'organizzazione per gli utenti di quel profilo. Le modifiche al `Valore timeout` dell'organizzazione non saranno valide per gli utenti di un profilo dotato di un proprio valore Timeout sessione.

1. Da Imposta, immettere *Profili* nella casella `Ricerca veloce`, quindi selezionare **Profili**.
2. Selezionare un profilo.
3. A seconda dell'interfaccia utente utilizzata, eseguire una delle seguenti operazioni:
   - Interfaccia utente profilo ottimizzata: fare clic su **Timeout sessione** e quindi su **Modifica**.
   - Interfaccia utente profilo originale: fare clic su **Modifica**, quindi far scorrere l'elenco fino alla sezione Timeout sessione.
4. Selezionare un valore di timeout dall'elenco a discesa.
5. Fare clic su **Salva**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni delle sessioni e delle password nei profili:
- "Gestisci profili e insiemi di autorizzazioni"

## Visualizzazione e modifica dei criteri relativi alle password nei profili

Per garantire un livello di sicurezza delle password adeguato all'interno dell'organizzazione, specificare i requisiti delle password nelle impostazioni dei criteri relativi alle password. Per gli utenti valgono i criteri relativi alle password stabiliti per l'intera organizzazione, fino a quando non si impostano tali criteri nel profilo stesso. Una volta configurate, le impostazioni delle password di un profilo hanno la precedenza sui criteri relativi alle password dell'organizzazione per gli utenti di quel profilo.

Le modifiche ai criteri relativi alle password dell'organizzazione non sono valide per gli utenti di un profilo dotato di criteri propri.

1. Da Imposta, immettere *Profili* nella casella `Ricerca veloce`, quindi selezionare **Profili**.
2. Selezionare un profilo.
3. A seconda dell'interfaccia utente utilizzata, eseguire una delle seguenti operazioni:
   - Interfaccia utente profilo ottimizzata: fare clic su **Criteri relativi alle password** e quindi su **Modifica**.
   - Interfaccia utente profilo originale: fare clic su **Modifica**, quindi far scorrere l'elenco fino alla sezione Criteri relativi alle password.
4. Modificare i valori del profilo.
5. Fare clic su **Salva**.

VEDERE ANCHE:

Campi dei criteri per le password nei profili

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni delle sessioni e delle password nei profili:
- "Gestisci profili e insiemi di autorizzazioni"

Per impostare i criteri di password:
- "Gestisci criteri relativi alle password"

## Campi dei criteri per le password nei profili

Specificare i requisiti delle password nelle impostazioni dei criteri relativi alle password. Fare riferimento a queste descrizioni dei campi per comprendere l'effetto dei singoli campi sui requisiti delle password di un profilo.

Le modifiche ai criteri relativi alle password dell'organizzazione non sono valide per gli utenti di un profilo dotato di criteri propri.

| Campo | Descrizione |
|---|---|
| `Le password utente scadono tra` | Periodo di tempo al termine del quale tutte le password utente scadono e devono essere cambiate. Questa impostazione non è valida per gli utenti in possesso dell'autorizzazione "La password non ha scadenza". Il valore predefinito è 90 giorni. Questa impostazione non è disponibile per i portali Self-Service. |
| `Memorizza le ultime password` | Consente di salvare le password precedenti degli utenti in modo che occorra sempre reimpostarle su un valore nuovo e univoco. La cronologia delle password non viene salvata finché non si imposta questo valore. Il valore predefinito è `3 password memorizzate`. Non è possibile selezionare l'opzione `Nessuna password memorizzata` a meno che per il campo `Le password utente scadono tra` non sia stata selezionata l'opzione `Nessuna scadenza`. Questa impostazione non è disponibile per i portali Self-Service. |
| `Lunghezza minima password` | Numero minimo di caratteri richiesti per una password. L'impostazione di questo valore non ha effetto sugli utenti esistenti finché non cambiano la propria password. Il valore predefinito è `8 caratteri`. |
| `Requisito di complessità password` | Requisito relativo ai tipi di caratteri che gli utenti possono utilizzare in una password.<br>Livelli di complessità:<br>• `Nessuna limitazione`: consente qualsiasi valore della password ed è l'opzione meno sicura.<br>• `Deve contenere caratteri alfanumerici`: richiede almeno un carattere alfabetico e un numero, che corrisponde all'impostazione predefinita.<br>• `Deve contenere caratteri alfanumerici e speciali`: richiede almeno un carattere alfabetico, un numero e uno dei seguenti caratteri: `! # $ % - _ = + < >`.<br>• `Deve contenere numeri e lettere maiuscole e minuscole`: richiede almeno un numero, un carattere alfabetico maiuscolo e uno minuscolo.<br>• `Deve contenere numeri, lettere maiuscole e minuscole e caratteri speciali`: richiede almeno un numero, un carattere alfabetico maiuscolo e uno minuscolo e uno dei seguenti caratteri: `! # $ % - _ = + < >`. |

| Campo | Descrizione |
| --- | --- |
| `Requisito domanda per la password` | I valori sono di tipo `Non può contenere la password`, ovvero la risposta alla domanda di suggerimento della password non può contenere la password, oppure di tipo `Nessuna`, l'impostazione predefinita, se non vi sono limitazioni relative alla risposta. È richiesta la risposta dell'utente alla domanda di suggerimento della password. Questa impostazione non è disponibile per i portali Self-Service, i Portali Clienti o i portali partner. |
| `Numero massimo di tentativi di accesso non validi` | Numero di accessi non riusciti consentiti a un utente prima che venga bloccato. Questa impostazione non è disponibile per i portali Self-Service. |
| `Periodo effettivo di blocco` | Durata del blocco dell'accesso. Il valore predefinito è 15 minuti. Questa impostazione non è disponibile per i portali Self-Service.<br><br>Nota: gli utenti il cui accesso è stato bloccato, devono aspettare la scadenza del periodo di blocco. In alternativa, un utente con l'autorizzazione "Reimposta password utente e sblocca utenti" può sbloccarli facendo clic su *`Utenti`* nella casella `Ricerca veloce`, quindi selezionando **Utenti**, selezionando l'utente e facendo clic su **Sblocca**. Questo pulsante è disponibile solo quando un utente è bloccato. |
| `Oscura risposta segreta per le reimpostazioni delle password` | Questa funzione consente di nascondere le risposte alle domande di sicurezza durante la digitazione. L'impostazione predefinita mostra la risposta come testo normale.<br><br>Nota: se l'organizzazione utilizza l'IME (Input Method Editor) Microsoft con la modalità di inserimento impostata su Hiragana, quando si digitano i caratteri ASCII essi vengono convertiti in caratteri giapponesi nei campi di testo normale. Tuttavia, l'IME non funziona correttamente nei campi con testo oscurato. Se gli utenti dell'organizzazione non riescono a immettere correttamente le loro password o altri valori dopo l'abilitazione di questa funzione, disabilitarla. |
| `Richiedi una durata della password di almeno 1 giorno` | Quando si seleziona questa opzione, una password non può essere modificata più di una volta nell'arco di 24 ore. |

VEDERE ANCHE:

Visualizzazione e modifica dei criteri relativi alle password nei profili

# Insiemi di autorizzazioni

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Un insieme di autorizzazioni è una raccolta di impostazioni e autorizzazioni che consente all'utente di accedere a vari strumenti e funzioni. Le impostazioni e le autorizzazioni negli insiemi di autorizzazioni sono contenute anche nei profili, ma gli insiemi di autorizzazioni estendono l'accesso funzionale degli utenti senza modificare il loro profilo.

Gli utenti possono avere un solo profilo, ma più insiemi di autorizzazioni. Gli insiemi di autorizzazioni possono essere assegnati a vari tipi di utenti, indipendentemente dai loro profili.

Nota: Nelle versioni Contact Manager Edition, Group Edition e Professional Edition è possibile creare un solo insieme di autorizzazioni.

Se un'autorizzazione non è abilitata in un profilo ma è abilitata in un insieme di autorizzazioni, l'utente con quel profilo e quell'insieme di autorizzazioni disporrà dell'autorizzazione. Ad esempio, se "Gestisci criteri relativi alle password" non è abilitata nel profilo di Jane Smith ma è abilitaa in uno dei suoi insiemi di autorizzazioni, Jane Smith potrà gestire i criteri relativi alle password.

Utilizzare gli insiemi di autorizzazioni per concedere l'accesso a raggruppamenti logici di utenti, indipendentemente dalla loro qualifica principale. Si supponga ad esempio di disporre di un oggetto personalizzato Inventario nella propria organizzazione. Numerosi utenti necessitano dell'accesso "Lettura" all'oggetto mentre un numero limitato di utenti necessita dell'accesso "Modifica". Per soddisfare questa esigenza, è possibile creare un insieme di autorizzazioni che concede l'accesso "Lettura" e assegnarlo agli utenti appropriati. È possibile creare un altro insieme di autorizzazioni che concede l'accesso "Modifica" all'oggetto Inventario e assegnarlo al gruppo di utenti più piccolo.

Guarda una dimostrazione: Creazione, modifica e assegnazione di un insieme di autorizzazioni

VEDERE ANCHE:

Modifica di insiemi di autorizzazioni da una visualizzazione elenco
Assegnare insiemi di autorizzazioni a un unico utente
Considerazioni sugli insiemi di autorizzazioni
Autorizzazioni utente per Crittografia piattaforma
Creazione di un segreto tenant
Autorizzazioni utente per Crittografia piattaforma
Creazione di un segreto tenant

## Creazione di insiemi di autorizzazioni

È possibile clonare un insieme di autorizzazioni esistente o crearne uno nuovo. Un insieme di autorizzazioni clonato include la stessa licenza utente e le stesse autorizzazioni abilitate dell'insieme da cui è stato clonato. Un nuovo insieme di autorizzazioni non include alcuna licenza utente selezionata né alcuna autorizzazione abilitata.

Guarda una dimostrazione: Creazione, modifica e assegnazione di un insieme di autorizzazioni

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per creare gli insiemi di autorizzazioni:

- "Gestisci profili e insiemi di autorizzazioni"

### Licenze utente negli insiemi di autorizzazioni

Quando si crea un insieme di autorizzazioni, è possibile selezionare una licenza utente specifica o **--Nessuno--**.

Se si seleziona una licenza specifica, scegliere quella che corrisponde agli utenti che utilizzano l'insieme di autorizzazioni. Ad esempio, se si prevede di assegnare l'insieme di autorizzazioni agli utenti con licenza Salesforce, selezionare Salesforce.

Se si prevede di assegnare l'insieme di autorizzazioni a più utenti con licenze diverse, selezionare **--Nessuno--** per non specificare alcuna licenza utente. Con questa opzione, è possibile assegnare l'insieme di autorizzazioni a qualsiasi utente la cui licenza consente le autorizzazioni abilitate. Ad esempio, se si prevede di assegnare l'insieme di autorizzazioni a utenti con licenza Salesforce e a utenti con licenza Salesforce Platform, selezionare **--Nessuno--**.

Nota:

- Gli insiemi di autorizzazioni senza licenza utente non prevedono tutte le autorizzazioni e le impostazioni possibili.
- È possibile assegnare un insieme di autorizzazioni senza licenza utente solo agli utenti le cui licenze consentono le autorizzazioni e impostazioni abilitate. Ad esempio, se si crea un insieme di autorizzazioni senza licenza utente e si abilita "Apex autore", non sarà possibile assegnare tale insieme di autorizzazioni agli utenti con licenza utente Salesforce Platform poiché la licenza non prevede tale autorizzazione.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

## Considerazioni sugli insiemi di autorizzazioni

Tenere presente le seguenti considerazioni e comportamenti speciali relativi agli insiemi di autorizzazioni.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

**Differenze tra gli insiemi di autorizzazioni nuovi e clonati**

Un nuovo insieme di autorizzazioni non include alcuna licenza utente selezionata né alcuna autorizzazione abilitata. Un insieme di autorizzazioni clonato include la stessa licenza utente e le stesse autorizzazioni abilitate dell'insieme da cui è stato clonato. Non è possibile modificare la licenza utente in un insieme di autorizzazioni clonato. Clonare un insieme di autorizzazioni solo se il nuovo insieme richiede la stessa licenza utente dell'originale.

**Limiti**

Nelle versioni Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition e Database.com Edition è possibile creare fino a 1.000 insiemi di autorizzazioni. Nelle versioni Contact Manager Edition, Group Edition e Professional Edition è possibile creare un solo insieme di autorizzazioni.

Nelle versioni Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition e Database.com Edition, le organizzazioni possono avere un numero maggiore di insiemi di autorizzazioni se questi vengono aggiunti come parte di un pacchetto gestito installato elencato pubblicamente su AppExchange. In questo caso, le organizzazioni possono avere fino a 1.500 insiemi di autorizzazioni.

**Limitazioni delle licenze utente**

Alcune licenze utente limitano il numero delle applicazioni o schede personalizzate a cui un utente può accedere. In questo caso, è possibile assegnare soltanto il numero assegnato attraverso il profilo e gli insiemi di autorizzazioni assegnati dell'utente. Ad esempio, un utente con licenza utente Force.com App Subscription dotato di accesso a una applicazione Force.com Light può accedere solo alle schede personalizzate di quell'applicazione.

**Applicazioni assegnate**

Le impostazioni delle applicazioni assegnate specificano le applicazioni che gli utenti possono selezionare nel menu delle applicazioni Force.com. Al contrario di quanto avviene per i profili, non è possibile assegnare un'applicazione predefinita negli insiemi di autorizzazioni. È possibile solo specificare se le applicazioni sono visibili.

**accesso classe Apex**

È possibile specificare quali metodi in una classe Apex di massimo livello sono eseguibili per un insieme di autorizzazioni. Le impostazioni di accesso della classe Apex possono essere applicate solo a:

- Metodi di classe Apex, ad esempio metodi di servizi Web
- Qualsiasi metodo utilizzato in un controller Visualforce personalizzato o un'estensione del controller applicata a una pagina Visualforce

I trigger vengono sempre attivati in caso di eventi trigger (quali `insert` o `update`) indipendentemente dalle impostazioni delle autorizzazioni.

VEDERE ANCHE:

Come viene specificato l'accesso ai tipi di record?

Licenze utente negli insiemi di autorizzazioni

Autorizzazioni sugli oggetti

## Utilizzo degli elenchi di insiemi di autorizzazioni

Per visualizzare gli insiemi di autorizzazioni della propria organizzazione, da Imposta immettere *Insiemi di autorizzazioni* nella casella `Ricerca veloce`, quindi selezionare **Insiemi di autorizzazioni**. Nella pagina dell'elenco di insiemi di autorizzazioni è possibile:

- Visualizzare un elenco filtrato di insiemi di autorizzazioni selezionando una visualizzazione dall'elenco a discesa.
- Creare una visualizzazione elenco o modificare una visualizzazione esistente
- Per eliminare una visualizzazione elenco, selezionarla dall'elenco a discesa e fare clic su **Elimina**.
- Creare un insieme di autorizzazioni facendo clic su **Crea**
- Stampare una visualizzazione elenco facendo clic su .
- Aggiornare la visualizzazione elenco facendo clic sull'
- Modificare le autorizzazioni direttamente nella visualizzazione elenco
- Visualizzare o modificare un insieme di autorizzazioni facendo clic sul nome
- Se non è assegnato ad alcun utente, rimuovere un insieme di autorizzazioni facendo clic su **Elimina**

VEDERE ANCHE:

Insiemi di autorizzazioni

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare gli insiemi di autorizzazioni e stampare gli elenchi di insiemi di autorizzazioni:

- "Visualizza impostazione e configurazione"

Per eliminare gli insiemi di autorizzazioni e le visualizzazioni di elenchi di insiemi di autorizzazioni:

- "Gestisci profili e insiemi di autorizzazioni"

## Creazione e modifica di visualizzazioni elenco di insiemi di autorizzazioni

È possibile creare e modificare visualizzazioni elenco degli insiemi di autorizzazioni per visualizzare un elenco di insiemi di autorizzazioni con autorizzazioni e campi specifici. Ad esempio, è possibile creare una visualizzazione elenco di tutti gli insiemi di autorizzazioni in cui è abilitata l'autorizzazione "Modifica tutti i dati".

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per creare, modificare ed eliminare visualizzazioni elenco di insiemi di autorizzazioni:

- "Gestisci profili e insiemi di autorizzazioni"

1. Nella pagina Insiemi di autorizzazioni, fare clic su **Crea nuova visualizzazione** o selezionare una visualizzazione e fare clic su **Modifica**.
2. Immettere il nome della visualizzazione.
3. In Specifica i criteri di filtro, specificare le condizioni a cui gli elementi dell'elenco devono corrispondere, ad esempio *Modifica tutti i dati uguale a Vero*.
   a. Digitare il nome di un'impostazione o fare clic su per cercare e selezionare l'impostazione desiderata.
   b. Scegliere un operatore filtro.
   c. Immettere il valore per la corrispondenza.

      Suggerimento: Per visualizzare solo gli insiemi di autorizzazioni senza licenza utente, inserire *Licenza utente* per `Impostazione`, impostare l'`Operatore` su *uguale a* e digitare *""* nel campo `Valore`.

   d. Per specificare un'altra condizione di filtro, fare clic su **Aggiungi riga**. È possibile specificare fino a 25 righe di condizioni di filtro.
4. In Seleziona le colonne da visualizzare, specificare le impostazioni che si desidera appaiano come colonne nella visualizzazione elenco. È possibile aggiungere fino a 15 colonne.
   a. Selezionare un tipo di impostazione dall'elenco a discesa Cerca.
   b. Immettere le prime lettere dell'impostazione che si desidera aggiungere e fare clic su **Trova**.

      Nota: se la ricerca trova più di 500 valori, non viene visualizzato alcun risultato. Perfezionare i criteri di ricerca per visualizzare un numero inferiore di risultati.

5. Fare clic su **Salva** oppure, se si sta clonando una visualizzazione esistente, rinominarla e fare clic su **Salva con nome**.

VEDERE ANCHE:

Modifica di insiemi di autorizzazioni da una visualizzazione elenco

## Modifica di insiemi di autorizzazioni da una visualizzazione elenco

È possibile modificare le autorizzazioni in un massimo di 200 insiemi di autorizzazioni direttamente dalla visualizzazione elenco, senza accedere ai singoli insiemi.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per modificare più insiemi di autorizzazioni dalla visualizzazione elenco:
- "Gestisci profili e insiemi di autorizzazioni"

Nota: prestare molta attenzione quando si utilizza questo metodo per modificare gli insiemi di autorizzazioni. Le modifiche globali potrebbero avere un effetto generale sugli utenti dell'organizzazione.

1. Selezionare o creare una visualizzazione elenco che includa gli insiemi di autorizzazioni e le autorizzazioni che si desidera modificare.
2. Per modificare più insiemi di autorizzazioni, selezionare la casella di controllo accanto a ciascun insieme da modificare. Se si selezionano insiemi di autorizzazioni su più pagine, verranno memorizzate le selezioni eseguite su ogni pagina.
3. Fare doppio clic sull'autorizzazione da modificare. Per più insiemi di autorizzazioni, fare doppio clic sull'autorizzazione in uno degli insiemi selezionati.
4. Nella finestra di dialogo visualizzata, abilitare o disabilitare l'autorizzazione. In alcuni casi, la modifica di un'autorizzazione può comportare la modifica di altre autorizzazioni. Ad esempio, se "Gestisci casi" e "Trasferisci casi" sono abilitate in un insieme di autorizzazioni e si disabilita "Trasferisci casi", viene disabilitata anche "Gestisci casi". In tal caso la finestra di dialogo elenca le autorizzazioni interessate.
5. Per modificare più insiemi di autorizzazioni, selezionare **Tutti i** *n* **record selezionati** (dove *n* è il numero di insiemi selezionati).
6. Fare clic su **Salva**.

Se si modificano più insiemi di autorizzazioni, verranno modificati solo quelli che supportano l'autorizzazione in corso di modifica. Si supponga ad esempio di utilizzare la modifica in linea per abilitare "Modifica tutti i dati" in dieci insiemi di autorizzazioni e che un insieme non includa "Modifica tutti i dati". In questo caso, "Modifica tutti i dati" viene abilitata in tutti gli insiemi di autorizzazioni, ad eccezione dell'insieme che non dispone dell'autorizzazione.

Eventuali modifiche apportate vengono registrate nell'itinerario di controllo delle impostazioni.

## Pagina Panoramica sull'insieme di autorizzazioni

La pagina della panoramica di un insieme di autorizzazioni costituisce un punto di accesso a tutte le autorizzazioni contenute nell'insieme. Per aprire la pagina della panoramica di un insieme di autorizzazioni, da Imposta immettere `Insiemi di autorizzazioni` nella casella `Ricerca veloce`, fare clic su **Insiemi di autorizzazioni** e selezionare l'insieme di autorizzazioni da visualizzare.

Guarda una dimostrazione: Creazione, modifica e assegnazione di un insieme di autorizzazioni

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per eliminare gli insiemi di autorizzazioni e modificare le proprietà degli insiemi di autorizzazioni:

- "Gestisci profili e insiemi di autorizzazioni"

## Informazioni sulle impostazioni delle applicazioni e di sistema negli insiemi di autorizzazioni

Negli insiemi di autorizzazioni, impostazioni e autorizzazioni sono suddivise nelle categorie applicazioni e sistema, che rispecchiano le autorizzazioni richieste agli utenti per amministrare e utilizzare le applicazioni e le risorse del sistema.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

### Impostazioni applicazione

Le applicazioni sono gruppi di schede che gli utenti possono modificare selezionando il menu a discesa nell'intestazione. Tutti gli oggetti, i componenti, i dati e le configurazioni sottostanti restano invariati, indipendentemente dall'applicazione selezionata. Con la selezione di un'applicazione, gli utenti si spostano in un gruppo di schede che consentono di utilizzare in modo efficiente le funzionalità sottostanti per le operazioni specifiche di un'applicazione. Si immagini ad esempio di svolgere la maggior parte del proprio lavoro nell'applicazione di vendita, che contiene schede come Account e Opportunità. Per monitorare una nuova campagna di marketing, anziché aggiungere la scheda Campagne all'applicazione di vendita è possibile selezionare Marketing dal menu a discesa delle applicazioni per visualizzare le proprie campagne e i relativi membri.

La sezione Applicazioni della pagina con la panoramica sugli insiemi di autorizzazioni contiene impostazioni direttamente associate ai processi aziendali resi possibili dalle applicazioni. Ad esempio, gli agenti dell'assistenza clienti potrebbero avere necessità di gestire i casi, per cui l'autorizzazione "Gestisci casi" si trova nella sezione Call Center della pagina Autorizzazioni applicazione. Alcune impostazioni delle applicazioni non sono correlate alle autorizzazioni applicazione. Ad esempio, per abilitare l'applicazione di gestione dei permessi da AppExchange, gli utenti devono poter accedere alle classi Apex e alle pagine Visualforce appropriate, nonché disporre delle autorizzazioni oggetti e campi che consentono di creare nuove richieste di permessi.

### Impostazioni di sistema

Alcune funzioni del sistema sono valide per l'organizzazione anziché per una singola applicazione. Ad esempio, "Visualizza impostazione e configurazione" consente agli utenti di visualizzare le pagine delle impostazioni di installazione e amministrazione. Altre funzioni del sistema sono valide per tutte le applicazioni. Ad esempio, le autorizzazioni "Esegui rapporti" e "Gestisci cruscotti digitali" permettono ai responsabili di creare e gestire rapporti in tutte le applicazioni. In alcuni casi, ad esempio con "Modifica tutti i dati", un'autorizzazione è valida per tutte le applicazioni ma comprende anche funzioni che esulano da queste ultime come la possibilità di scaricare Data Loader.

## Ricerca degli insiemi di autorizzazioni

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per eseguire una ricerca negli insiemi di autorizzazioni:

- "Visualizza impostazione e configurazione"

Per passare rapidamente ad altre pagine in un insieme di autorizzazioni, è possibile immettere termini di ricerca in qualsiasi pagina dei dettagli dell'insieme.

Nella pagina dei dettagli di un insieme di autorizzazioni, digitare almeno tre lettere consecutive del nome di un oggetto, di un'impostazione o di un'autorizzazione nella casella **Trova impostazioni...**. I termini della ricerca non fanno distinzione tra caratteri maiuscoli e minuscoli. Via via che si digitano i caratteri, vengono elencati i suggerimenti relativi ai risultati corrispondenti ai termini di ricerca inseriti. Fare clic su una voce dell'elenco per accedere alla relativa pagina delle impostazioni.

Per alcune categorie, è possibile cercare il nome dell'autorizzazione o dell'impostazione specifica. Per le altre categorie, eseguire la ricerca per nome di categoria.

| Voce | Ricerca di | Esempio |
|---|---|---|
| Applicazioni assegnate | Nome applicazione | Digitare *`vendite`* nella casella Trova impostazioni e selezionare `Vendite` dall'elenco. |
| Oggetti | Nome oggetto | Si supponga di avere un oggetto personalizzato denominato Album. Digitare *`albu`*, quindi selezionare `Album`. |
| • Campi<br>• Tipi di record | Nome oggetto principale | Si supponga che l'oggetto Album contenga un campo Descrizione. Per trovare il campo `Descrizione` tra gli album, digitare *`albu`*, selezionare `Album` e scorrere verso il basso fino a `Descrizione` in Autorizzazioni campi. |
| Schede | Nome scheda o oggetto principale | Digitare *`rap`* e quindi selezionare `Rapporti`. |
| Autorizzazioni di applicazioni e sistema | Nome autorizzazione | Digitare *`api`* e selezionare `API abilitata`. |
| Tutte le altre categorie | Nome categoria | Per trovare le impostazioni di accesso della classe Apex, digitare *`apex`*, quindi selezionare `Accesso classe Apex`. Per trovare le autorizzazioni personalizzate, digitare *`pers`*, quindi selezionare `Autorizzazioni personalizzate`. E così via. |

Se nella ricerca non appaiono risultati:

- Assicurarsi che il termine della ricerca contenga almeno tre caratteri consecutivi corrispondenti al nome dell'oggetto, dell'impostazione o dell'autorizzazione.
- Controllare che l'ortografia del termine cercato sia corretta.
- L'autorizzazione, l'oggetto o l'impostazione che si sta cercando potrebbe non essere disponibile nell'organizzazione corrente.
- La voce che si sta cercando potrebbe non essere disponibile per la licenza utente associata all'insieme di autorizzazioni corrente. Ad esempio, un insieme di autorizzazioni con licenza Utente Platform standard non include l'autorizzazione "Modifica tutti i dati".

VEDERE ANCHE:

Insiemi di autorizzazioni

## Visualizzazione e modifica delle applicazioni assegnate negli insiemi di autorizzazioni

Le impostazioni delle applicazioni assegnate specificano le applicazioni che gli utenti possono selezionare nel menu delle applicazioni Force.com.

Al contrario di quanto avviene per i profili, non è possibile assegnare un'applicazione predefinita negli insiemi di autorizzazioni. È possibile solo specificare se le applicazioni sono visibili.

Per assegnare le applicazioni:

1. Da Imposta, immettere *Insiemi di autorizzazioni* nella casella `Ricerca veloce`, quindi selezionare **Insiemi di autorizzazioni**.
2. Selezionare un insieme di autorizzazioni o crearne uno.
3. Nella pagina della panoramica dell'insieme di autorizzazioni, fare clic su **Applicazioni assegnate**.
4. Fare clic su **Modifica**.
5. Per assegnare le applicazioni, selezionarle dall'elenco Applicazioni disponibili e fare clic su **Aggiungi**. Per rimuovere le applicazioni dall'insieme di autorizzazioni, selezionarle dall'elenco Applicazioni abilitate e fare clic su **Rimuovi**.
6. Fare clic su **Salva**.

VEDERE ANCHE:

Insiemi di autorizzazioni

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni delle applicazioni assegnate:

- "Gestisci profili e insiemi di autorizzazioni"

## Assegnazione di tipi di record personalizzati negli insiemi di autorizzazioni

1. Da Imposta, immettere *Insiemi di autorizzazioni* nella casella `Ricerca veloce`, quindi selezionare **Insiemi di autorizzazioni**.
2. Selezionare un insieme di autorizzazioni o crearne uno.
3. Nella pagina della panoramica dell'insieme di autorizzazioni, fare clic su **Impostazioni oggetti** e quindi sull'oggetto desiderato.
4. Fare clic su **Modifica**.
5. Selezionare i tipi di record da assegnare a quell'insieme di autorizzazioni.
6. Fare clic su **Salva**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per assegnare i tipi di record negli insiemi di autorizzazioni:
- "Gestisci profili e insiemi di autorizzazioni"

VEDERE ANCHE:

Come viene specificato l'accesso ai tipi di record?

## Come viene specificato l'accesso ai tipi di record?

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

I tipi di record si possono assegnare agli utenti dai rispettivi profili o insiemi di autorizzazioni o da una combinazione di entrambi. L'assegnazione dei tipi di record funziona in modo diverso nei profili e negli insiemi di autorizzazioni.

- Il tipo di record predefinito di un utente è specificato nelle impostazioni personali dell'utente. Non è possibile specificare un tipo di record predefinito negli insiemi di autorizzazioni.
- È possibile assegnare nei profili il tipo di record `--Principale--`. Negli insiemi di autorizzazioni è possibile assegnare soltanto tipi di record personalizzati. La modalità di creazione dei record varia a seconda dei tipi di record assegnati nei profili e negli insiemi di autorizzazioni.

| Se nel profilo dell'utente è assegnato questo tipo di record... | E l'insieme di autorizzazioni include il seguente numero di tipi di record personalizzati... | Quando l'utente crea un record... |
| --- | --- | --- |
| `--Principale--` | Nessuno | Il nuovo record viene associato al tipo di record Principale |
| `--Principale--` | Uno | Il nuovo record viene associato al tipo di record personalizzato. L'utente non può selezionare il tipo di record Principale. |
| `--Principale--` | Più di uno | All'utente viene richiesto di selezionare un tipo di record. |

| Se nel profilo dell'utente è assegnato questo tipo di record... | E l'insieme di autorizzazioni include il seguente numero di tipi di record personalizzati... | Quando l'utente crea un record... |
|---|---|---|
| Personalizzato | Uno o più di uno | All'utente viene richiesto di selezionare un tipo di record. Nelle impostazioni personali, gli utenti possono impostare l'uso del tipo di record predefinito per evitare di dover scegliere un tipo di record. |

- Le assegnazioni dei layout di pagina sono specificate solo nei profili e non sono disponibili negli insiemi di autorizzazioni. Quando un insieme di autorizzazioni specifica un tipo di record personalizzato, agli utenti con quell'insieme di autorizzazioni viene assegnato il layout di pagina specificato per quel tipo di record nei rispettivi profili. (nei profili, le assegnazioni dei layout di pagina sono specificate per ogni tipo di record, anche quando i tipi di record non sono assegnati).
- Per la conversione dei lead, per i record convertiti viene utilizzato il tipo di record predefinito specificato nel profilo dell'utente.
- Gli utenti possono visualizzare i record assegnati a qualsiasi tipo di record. Di conseguenza, a ogni tipo di record nel profilo di un utente viene assegnato un layout di pagina. L'assegnazione di un tipo di record nel profilo o nell'insieme di autorizzazioni di un utente non determina la visualizzazione dei record con quel tipo di record per l'utente. L'assegnazione del tipo di record specifica semplicemente che l'utente può utilizzare quel tipo di record durante la creazione o la modifica di un record.
- I tipi di record negli insiemi di autorizzazioni non sono supportati nei pacchetti e nelle serie di modifiche. Di conseguenza, tutte le assegnazioni di tipi di record negli insiemi di autorizzazioni di un'organizzazione Sandbox devono essere riprodotte manualmente nell'organizzazione di produzione.

VEDERE ANCHE:

Assegnazione dei tipi di record e dei layout di pagina nell'interfaccia utente profilo ottimizzata

Assegnazione di tipi di record ai profili nell'interfaccia utente profilo originale

Assegnazione di tipi di record personalizzati negli insiemi di autorizzazioni

Assegnazione dei layout di pagina nell'interfaccia utente profilo originale

## Abilitazione di autorizzazioni personalizzate negli insiemi di autorizzazioni

Le autorizzazioni personalizzate rappresentano un modo per consentire l'accesso a processi o applicazioni personalizzate. Dopo avere creato un'autorizzazione personalizzata e averla associata a un processo o a un'applicazione, è possibile abilitarla negli insiemi di autorizzazioni.

1. Da Imposta, immettere *Insiemi di autorizzazioni* nella casella `Ricerca veloce`, quindi selezionare **Insiemi di autorizzazioni**.
2. Selezionare un insieme di autorizzazioni o crearne uno.
3. Nella pagina della panoramica dell'insieme di autorizzazioni, fare clic su **Autorizzazioni personalizzate**.
4. Fare clic su **Modifica**.
5. Per abilitare le autorizzazioni personalizzate, selezionarle dall'elenco Autorizzazioni personalizzate disponibili e fare clic su **Aggiungi**. Per rimuovere le autorizzazioni personalizzate dall'insieme di autorizzazioni, selezionarle dall'elenco Autorizzazioni personalizzate abilitate e fare clic su **Rimuovi**.
6. Fare clic su **Salva**.

EDIZIONI

Disponibile nella versione: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Nelle organizzazioni Group Edition e Professional Edition non è possibile creare o modificare le autorizzazioni personalizzate, ma è possibile installarle come parte di un pacchetto gestito.

AUTORIZZAZIONI UTENTE

Per abilitare le autorizzazioni personalizzate negli insiemi di autorizzazioni:

- "Gestisci profili e insiemi di autorizzazioni"

## Gestione di assegnazioni di insiemi di autorizzazioni

È possibile assegnare insiemi di autorizzazioni a un unico utente dalla pagina dei dettagli dell'utente o assegnare più utenti a un insieme di autorizzazioni da qualsiasi pagina dell'insieme di autorizzazioni.

- Assegnare insiemi di autorizzazioni a un unico utente
- Assegnare un insieme di autorizzazioni a più utenti
- Rimuovere le assegnazioni utente da un insieme di autorizzazioni

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

## Pagina utenti assegnati all'insieme di autorizzazioni

Dalla pagina Utenti assegnati, è possibile visualizzare tutti gli utenti assegnati a un insieme di autorizzazioni, assegnare ulteriori utenti e rimuovere le assegnazioni utente.

Per visualizzare tutti gli utenti assegnati a un insieme di autorizzazioni, da qualsiasi pagina dell'insieme di autorizzazioni, fare clic su **Gestisci assegnazioni**. Dalla pagina Utenti assegnati è possibile:

- Assegnare utenti all'insieme di autorizzazioni
- Rimuovere le assegnazioni utente dall'insieme di autorizzazioni
- Modificare un utente
- Visualizzare la pagina dei dettagli di un utente facendo clic sul nome, sull'alias o sul nome utente
- Visualizzare un profilo facendo clic sul nome del profilo

VEDERE ANCHE:

Assegnare insiemi di autorizzazioni a un unico utente

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare gli utenti assegnati a un insieme di autorizzazioni:

- "Visualizza impostazione e configurazione"

## Assegnare insiemi di autorizzazioni a un unico utente

Dalla pagina dei dettagli dell'utente è possibile assegnare insiemi di autorizzazioni o rimuovere le assegnazioni di insiemi di autorizzazioni per un unico utente.

1. Da Imposta, immettere *`Utenti`* nella casella `Ricerca veloce`, quindi selezionare **Utenti**.
2. Selezionare un utente.
3. Nell'elenco correlato Assegnazioni dell'insieme di autorizzazioni, fare clic su **Modifica assegnazioni**.
4. Per assegnare un insieme di autorizzazioni, selezionarlo dalla casella Insiemi di autorizzazioni disponibili e fare clic su **Aggiungi**. Per rimuovere l'assegnazione di un insieme di autorizzazioni, selezionarla dalla casella Insiemi di autorizzazioni abilitati e fare clic su **Rimuovi**.

   Nota:

   - Nella pagina Assegnazioni dell'insieme di autorizzazioni figurano gli insiemi di autorizzazioni a cui non sono associate licenze e quelli che corrispondono alla licenza dell'utente. Ad esempio, se la licenza di un utente è Chatter Only, sarà possibile assegnare all'utente gli insiemi di autorizzazioni con licenza Chatter Only e quelli privi di licenze associate.

     Se si assegna un insieme di autorizzazioni sprovvisto di licenza utente, tutte le relative impostazioni e autorizzazioni abilitate devono essere consentite dalla licenza dell'utente: in caso contrario l'assegnazione non andrà a buon fine.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per assegnare gli insiemi di autorizzazioni:

- "Assegna insiemi di autorizzazioni"

- Per alcune autorizzazioni, gli utenti devono disporre di *licenze insieme di autorizzazioni* prima di potere avere tali autorizzazioni. Ad esempio, se si aggiunge l'autorizzazione "Utilizza Identity Connect" all'insieme di autorizzazioni "Identità", solo gli utenti con la licenza insieme di autorizzazioni Identity Connect possono vedersi assegnare l'insieme di autorizzazioni "Identità".

5. Fare clic su **Salva**.

Suggerimento: questa e altre operazioni di amministrazione possono essere eseguite dall'app mobile SalesforceA.

VEDERE ANCHE:

Assegnare un insieme di autorizzazioni a più utenti

SalesforceA

Licenze utente negli insiemi di autorizzazioni

Assegnare un insieme di autorizzazioni a più utenti

## Assegnare un insieme di autorizzazioni a più utenti

Da qualsiasi pagina dell'insieme di autorizzazioni è possibile assegnare l'insieme a uno o più utenti.

- Guarda una dimostrazione: assegnare un insieme di autorizzazioni

VEDERE ANCHE:

Rimuovere le assegnazioni utente da un insieme di autorizzazioni

Assegnare insiemi di autorizzazioni a un unico utente

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per assegnare un insieme di autorizzazioni agli utenti:

- "Assegna insiemi di autorizzazioni"

## Rimuovere le assegnazioni utente da un insieme di autorizzazioni

Da qualsiasi pagina dell'insieme di autorizzazioni è possibile rimuovere da uno o più utenti l'assegnazione a un insieme di autorizzazioni.

1. Da Imposta, immettere *Insiemi di autorizzazioni* nella casella Ricerca veloce, quindi selezionare **Insiemi di autorizzazioni**.
2. Selezionare un insieme di autorizzazioni.
3. Nella barra degli strumenti dell'insieme di autorizzazioni, fare clic su **Gestisci assegnazioni**.
4. Selezionare gli utenti da rimuovere dall'insieme di autorizzazioni.

   È possibile rimuovere un massimo di 1000 utenti alla volta.
5. Fare clic su **Rimuovi assegnazioni**.

   Questo pulsante è disponibile solo quando è stato selezionato almeno un utente.
6. Per tornare a un elenco di tutti gli utenti assegnati all'insieme di autorizzazioni, fare clic su **Chiudi**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per rimuovere le assegnazioni di insiemi di autorizzazioni:
- "Assegna insiemi di autorizzazioni"

VEDERE ANCHE:

Assegnare un insieme di autorizzazioni a più utenti

# Revoca di autorizzazioni e accesso

È possibile utilizzare i profili e gli insiemi di autorizzazioni per concedere l'accesso ma non per negarlo. Eventuali autorizzazioni concesse da un profilo o da un insieme di autorizzazioni devono essere rispettate. Se ad esempio l'autorizzazione "Trasferisci record" non è abilitata nel profilo di Giulia Siani ma lo è in due dei suoi insiemi di autorizzazioni, i record potranno essere trasferiti anche se Giulia Siani non ne è titolare. Per revocare un'autorizzazione, è necessario rimuovere tutte le istanze dell'autorizzazione dall'utente. Questa operazione può essere eseguita mediante le seguenti azioni, ciascuna delle quali prevede alcune conseguenze.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

| Azione | Conseguenza |
|---|---|
| Disabilitare un'autorizzazione o rimuovere un'impostazione di accesso nel profilo e in tutti gli insiemi di autorizzazioni assegnati all'utente. | L'autorizzazione o l'impostazione di accesso viene disabilitata per tutti gli altri utenti assegnati al profilo o agli insiemi di autorizzazioni. |
| Se un'autorizzazione o un'impostazione di accesso è abilitata nel profilo dell'utente, assegnare un profilo diverso all'utente<br>E<br>se l'autorizzazione o l'impostazione di accesso è abilitata in uno degli insiemi di autorizzazioni | L'utente può perdere altre autorizzazioni o impostazioni di accesso associate al profilo o agli insiemi di autorizzazioni. |

| Azione | Conseguenza |
| --- | --- |
| assegnati all'utente, rimuovere tali assegnazioni dall'utente. | |

Per ovviare alla conseguenza in entrambi i casi, considerare tutte le opzioni possibili. Ad esempio, è possibile clonare il profilo assegnato o gli eventuali insiemi di autorizzazioni assegnati in cui è abilitata l'autorizzazione o l'impostazione di accesso, disabilitare l'autorizzazione o l'impostazione di accesso e assegnare il profilo o gli insiemi di autorizzazioni clonati all'utente. Un'altra possibilità è creare un profilo di base con il numero minimo di autorizzazioni e impostazioni che rappresenti il massimo numero di utenti possibile, quindi creare insiemi di autorizzazioni che forniscano ulteriori possibilità di accesso.

VEDERE ANCHE:

Autorizzazioni e accesso degli utenti

Tour dimostrativo: creazione, modifica e assegnazione di un insieme di autorizzazioni

Assegnare insiemi di autorizzazioni a un unico utente

# Accesso ai campi

## Accessibilità dei campi

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

I layout di pagina non sono disponibili in **Database.com** Edition

Diversi fattori contribuiscono a controllare se gli utenti possono visualizzare e modificare determinati campi in Salesforce.

- **Layout di pagina** - È possibile impostare se i campi sono visibili, obbligatori, modificabili o di sola lettura.
- **Protezione livello campo** - È possibile limitare ulteriormente l'accesso degli utenti ai campi impostando se tali campi sono visibili, modificabili o di sola lettura. Tali impostazioni ignorano le proprietà dei campi impostate nel layout di pagina se la protezione a livello di campo è più restrittiva.

  Nota: La protezione a livello di campo non impedisce di effettuare ricerche sui valori di un campo. Quando i termini della ricerca corrispondono ai valori di campo con protezione a livello di campo, nei risultati della ricerca vengono restituiti i record associati senza i campi protetti e i relativi valori.

- **Autorizzazioni** - Alcune autorizzazioni utente ignorano sia i layout di pagina sia le impostazioni di protezione a livello di campo. Ad esempio, gli utenti che dispongono dell'autorizzazione per la modifica dei campi di sola lettura potranno sempre modificare i campi di sola lettura indipendentemente dalle altre impostazioni.
- **Campi universalmente obbligatori**—I campi personalizzati possono essere resi universalmente obbligatori; questa impostazione sovrascrive tutte le impostazioni meno restrittive dei layout di pagina o della protezione a livello di campo.

Dopo che sono stati impostati questi elementi, è possibile confermare l'accesso degli utenti ai campi specifici mediante la griglia di accessibilità dei campi.

VEDERE ANCHE:

Modifica delle impostazioni di accesso ai campi

## Verifica dell'accessibilità dei campi per un determinato campo

1. Accedere all'area dei campi dell'oggetto appropriato:
   - Per gli elenchi di selezione degli stati di convalida Knowledge, da Imposta immettere *Stati convalida* nella casella `Ricerca veloce`, quindi selezionare **Stati convalida**.
2. Selezionare un campo e fare clic su **Visualizza accessibilità campo**.
3. Verificare che l'accesso al campo sia corretto per i vari profili e tipi di record.
4. Passare il mouse sopra qualsiasi impostazione di accesso ai campi per vedere se il campo è obbligatorio, modificabile, nascosto o di sola lettura in base al layout di pagina o alla protezione a livello di campo.
5. Fare clic su qualsiasi impostazione di accesso ai campi per modificare l'accessibilità del campo.

Per le opzioni avanzate di verifica dell'accessibilità dei campi in base a uno specifico profilo, tipo di record o campo, da Imposta, immettere *Accessibilità campo* nella casella `Ricerca veloce`, quindi selezionare **Accessibilità campo**. Da questa pagina è necessario scegliere una scheda specifica da visualizzare e quindi decidere se verificare l'accesso in base a profili, tipi di record o campi.

Nota: in questa interfaccia utente, non è possibile verificare l'accesso per gli insiemi di autorizzazioni.

la protezione a livello di campo non impedisce di effettuare ricerche sui valori di un campo. Per impostare l'organizzazione in modo da impedire agli utenti di effettuare ricerche e recuperare record corrispondenti a un valore in un campo nascosto dalla protezione a livello di campo, rivolgersi all'assistenza clienti.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare l'accessibilità campo:
- "Visualizza impostazione e configurazione"

VEDERE ANCHE:

Accessibilità dei campi

## Modifica delle impostazioni di accesso ai campi

Dalla griglia di accessibilità ai campi, è possibile fare clic su qualsiasi impostazione di accesso a un campo per modificare l'accessibilità nel layout di pagina o nella protezione a livello di campo. Le impostazioni di accesso ai campi sono quindi modificabili nella pagina Impostazioni accesso.

- Nella sezione Protezione livello campo della pagina, specificare il livello di accesso del campo per il profilo.

| Livello di accesso | Impostazioni abilitate |
|---|---|
| Gli utenti possono leggere e modificare il campo. | **Visibile** |
| Gli utenti possono leggere il campo ma non modificarlo. | **Visibile** e **Sola lettura** |
| Gli utenti non possono leggere né modificare il campo. | Nessuno |

  Anziché creare più layout di pagina per controllare l'accesso ai campi, si consiglia di utilizzare una protezione a livello di campo.

- Nella sezione Layout di pagina della pagina è possibile:
  - Selezionare il pulsante di opzione `Rimuovere o modificare la possibilità di modifica`, quindi modificare le proprietà di accesso al campo per il layout di pagina. Tali modifiche riguarderanno tutte le combinazioni di profilo e tipo di record che utilizzano attualmente il layout di pagina selezionato.
  - In alternativa, è possibile selezionare il pulsante di opzione `Scegliere un altro layout di pagina` per assegnare un altro layout di pagina alla combinazione di profilo e tipo di record.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare l'accessibilità ai campi:
- "Visualizza impostazione e configurazione"

Per modificare l'accessibilità ai campi:
- "Personalizza applicazione"

  E

  "Gestisci profili e insiemi di autorizzazioni"

VEDERE ANCHE:

Accessibilità dei campi

## Panoramica sulla protezione a livello di campo

Le impostazioni di sicurezza a livello di campo consentono agli amministratori di limitare l'accesso degli utenti alla visualizzazione e alla modifica di determinati campi nei seguenti punti:

- Pagine dei dettagli e di modifica
- Elenchi correlati
- Visualizzazioni elenco
- Rapporti
- Connect Offline
- Modelli di email e di stampa unione
- Link personalizzati
- Portale partner

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

- Portale Clienti di Salesforce
- Dati sincronizzati
- Dati importati

I campi che sono visibili agli utenti nelle pagine dei dettagli e di modifica sono una combinazione delle impostazioni di protezione a livello di campo e dei layout di pagina. Vengono applicate sempre le impostazioni di accesso ai campi più restrittive. Ad esempio, se un campo è obbligatorio nel layout di pagina e di sola lettura nelle impostazioni di protezione a livello di campo, queste ultime avranno la precedenza e il campo sarà di sola lettura per l'utente.

Importante: La protezione a livello di campo non impedisce di effettuare ricerche sui valori di un campo. Quando i termini della ricerca corrispondono ai valori di campo con protezione a livello di campo, nei risultati della ricerca vengono restituiti i record associati senza i campi protetti e i relativi valori.

Per definire la protezione a livello di campo, procedere in uno dei seguenti modi:

- Per più campi in un unico insieme di autorizzazioni o profilo
- Per un unico campo in tutti i profili

Dopo aver impostato la protezione a livello di campo per gli utenti, è possibile:

- Creare layout di pagina per organizzare i campi nelle pagine dei dettagli e di modifica.
- Verificare l'accesso degli utenti ai campi controllando l'accessibilità dei campi.
- Personalizzare i layout di ricerca per impostare i campi che vengono visualizzati nei risultati delle ricerche, nei risultati delle ricerche nella finestra di dialogo di ricerca e negli elenchi chiave nelle pagine iniziali delle schede.

Nota: i campi formula e riepilogo di roll-up sono sempre di sola lettura nelle pagine dei dettagli e non sono disponibili nelle pagine di modifica. Possono inoltre essere visibili agli utenti anche se i campi a cui fanno riferimento non sono visibili. I campi universalmente obbligatori vengono sempre visualizzati nelle pagine di modifica indipendentemente dalla protezione a livello di campo.

La creazione guidata di gruppi relazione consente di creare e modificare i gruppi relazione indipendentemente dalla protezione a livello di campo.

## Impostazione delle autorizzazioni sui campi negli insiemi di autorizzazioni e nei profili

Le autorizzazioni sui campi specificano il livello di accesso per i singoli campi di un oggetto.

1. Da Imposta:
   - Immettere *Insiemi di autorizzazioni* nella casella `Ricerca veloce`, quindi selezionare **Insiemi di autorizzazioni** oppure
   - Immettere *Profili* nella casella `Ricerca veloce`, quindi selezionare **Profili**
2. Selezionare un insieme di autorizzazioni o un profilo.
3. A seconda dell'interfaccia utilizzata, eseguire una delle seguenti operazioni:
   - Insiemi di autorizzazioni o interfaccia utente profilo ottimizzata: nella casella **Trova impostazioni...**, digitare il nome dell'oggetto desiderato e selezionarlo dall'elenco. Fare clic su **Modifica**, quindi far scorrere l'elenco fino alla sezione Autorizzazioni campi.
   - Interfaccia utente profilo originale: nella sezione Protezione livello campo, fare clic su **Visualizza** accanto all'oggetto che si desidera modificare, quindi fare clic su **Modifica**.
4. Specificare il livello di accesso del campo.
5. Fare clic su **Salva**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per impostare la protezione a livello di campo:

- "Gestisci profili e insiemi di autorizzazioni"

  E

  "Personalizza applicazione"

## Impostazione della protezione a livello di campo per un unico campo in tutti i profili

1. Dalle impostazioni di gestione per l'oggetto del campo, accedere all'area dei campi.
2. Selezionare il campo che si desidera modificare.
3. Fare clic su **Visualizza accessibilità campo**.
4. Specificare il livello di accesso del campo.
5. Fare clic su **Salva**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per impostare la protezione a livello di campo:

- "Gestisci profili e insiemi di autorizzazioni"

  E

  "Personalizza applicazione"

# Riferimento Autorizzazioni

## Autorizzazioni utente

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Le autorizzazioni utente disponibili variano secondo la versione (Edition) utilizzata.

Le autorizzazioni utente specificano quali operazioni possono essere eseguite dagli utenti e a quali funzioni gli utenti hanno accesso. Ad esempio, gli utenti in possesso dell'autorizzazione "Visualizza impostazione e configurazione" possono visualizzare le pagine Imposta e gli utenti in possesso dell'autorizzazione "API abilitata" possono accedere a qualsiasi API Salesforce. È possibile attivare le autorizzazioni utente negli insiemi di autorizzazioni e nei profili personalizzati. Negli insiemi di autorizzazioni e nell'interfaccia utente profilo ottimizzata, queste autorizzazioni e le loro descrizioni sono elencate nelle pagine Autorizzazioni applicazione o Autorizzazioni di sistema. Nell'interfaccia utente profilo originale, le autorizzazioni utente sono invece elencate nelle Autorizzazioni amministrative e Autorizzazioni utente generali.

Per visualizzare le autorizzazioni e le relative descrizioni, da Imposta, immettere *`Insiemi di autorizzazioni`* nella casella `Ricerca veloce`, quindi selezionare **Insiemi di autorizzazioni** e selezionare o creare un insieme di autorizzazioni. Quindi, dalla pagina Panoramica sull'insieme di autorizzazioni, fare clic su **Autorizzazioni applicazione** o **Autorizzazioni di sistema**.

VEDERE ANCHE:

Profili

Insiemi di autorizzazioni

Profili standard

## Autorizzazioni sugli oggetti

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Le autorizzazioni sugli oggetti specificano l'accesso di base di cui dispongono gli utenti per creare, leggere, modificare ed eliminare record per ogni oggetto. Le autorizzazioni sugli oggetti si possono gestire negli insiemi di autorizzazioni e nei profili.

Le autorizzazioni oggetto possono rispettare o ignorare le regole e le impostazioni di condivisione. Le autorizzazioni che seguono specificano l'accesso agli oggetti di cui dispongono gli utenti.

| Autorizzazione | Descrizione | Rispetta o ignora la condivisione? |
|---|---|---|
| Lettura | Gli utenti possono solo visualizzare i record di questo tipo. | Rispetta la condivisione |
| Crea | Gli utenti possono visualizzare e creare record. | Rispetta la condivisione |
| Modifica | Gli utenti possono visualizzare e aggiornare i record. | Rispetta la condivisione |
| Elimina | Gli utenti possono visualizzare, modificare ed eliminare i record. | Rispetta la condivisione |
| Visualizza tutto | Gli utenti possono visualizzare tutti i record associati a questo oggetto, a prescindere dalle impostazioni di condivisione. | Ignora la condivisione |

| Autorizzazione | Descrizione | Rispetta o ignora la condivisione? |
|---|---|---|
| Modifica tutto | Gli utenti possono leggere, modificare, eliminare, trasferire e approvare tutti i record associati a questo oggetto, a prescindere dalle impostazioni di condivisione.<br>Nota: l'autorizzazione "Modifica tutto" riferita ai documenti consente di accedere a tutte le cartelle pubbliche e condivise, ma non di modificarne le proprietà o creare nuove cartelle. Per modificare le proprietà delle cartelle o creare nuove cartelle, gli utenti devono disporre dell'autorizzazione "Gestisci documenti pubblici". | Ignora la condivisione |

VEDERE ANCHE:

Panoramica sulle autorizzazioni "Visualizza tutto" e "Modifica tutto"

Confronto tra i modelli di protezione

Autorizzazioni sui campi

## Panoramica sulle autorizzazioni "Visualizza tutto" e "Modifica tutto"

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni

Le autorizzazioni “Visualizza tutto” e “Modifica tutto” ignorano le regole e le impostazioni di condivisione e consentono agli amministratori di concedere rapidamente accesso ai record associati a un determinato oggetto in tutta l'organizzazione. "Visualizza tutto" e "Modifica tutto" potrebbero essere alternative preferibili alle autorizzazioni "Visualizza tutti i dati" e "Modifica tutti i dati". Tenere presenti le seguenti distinzioni fra i vari tipi di autorizzazioni.

| Autorizzazioni | Utilizzate per | Utenti per cui sono necessarie |
|---|---|---|
| Visualizza tutto<br>Modifica tutto | Delega delle autorizzazioni oggetto | Amministratori delegati che devono gestire record di oggetti specifici. |
| Visualizza tutti i dati<br>Modifica tutti i dati | Gestione di tutti i dati di un'organizzazione; ad esempio pulizia dei dati, eliminazione di duplicati, eliminazione globale, trasferimento globale e gestione delle approvazioni dei record. | Amministratori di un'intera organizzazione |
| Visualizza tutti gli utenti | Visualizzazione di tutti gli utenti dell'organizzazione. Questa autorizzazione concede l'accesso in Lettura a tutti gli utenti e permette quindi di vedere i dettagli dei relativi record utente, di vedere gli utenti nelle ricerche, nelle visualizzazioni elenco e così via. | Utenti che devono poter vedere tutti gli utenti dell'organizzazione, soprattutto se l'impostazione predefinita dell'organizzazione per l'oggetto Utente è Privato. Agli amministratori dotati di autorizzazione "Gestisci utenti" viene assegnata automaticamente l'autorizzazione "Visualizza tutti gli utenti". |

"Visualizza tutto" e "Modifica tutto" non sono disponibili per idee, listini prezzi, tipi di articoli e prodotti.

"Visualizza tutto" e "Modifica tutto" consentono solo la delega delle autorizzazioni oggetto. Per delegare funzioni di amministrazione utenti e amministrazione oggetti personalizzati, definire degli amministratori delegati.

"Visualizza tutti gli utenti" è disponibile se l'organizzazione è dotata di Condivisioni utente, che controllano la visibilità degli utenti nell'organizzazione. Per informazioni sulle Condivisioni utente, vedere Panoramica sulle condivisioni utente.

VEDERE ANCHE:

Autorizzazioni sugli oggetti

## Confronto tra i modelli di protezione

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

La protezione degli utenti di Salesforce è una combinazione di condivisione e di autorizzazioni utente e oggetto. In alcuni casi, ad esempio per l'accesso a livello di record degli utenti finali, è utile utilizzare la condivisione per fornire l'accesso ai record. In altri casi, invece, ad esempio la delega di operazioni di amministrazione dei record quali il trasferimento di record, la pulizia dei dati, l'eliminazione dei record duplicati, l'eliminazione globale dei record e la delega dei processi di approvazione flusso di lavoro, è meglio ignorare la condivisione e utilizzare i profili per fornire l'accesso ai record.

Le autorizzazioni "Lettura", "Crea", "Modifica" ed "Elimina" rispettano le impostazioni di condivisione che controllano l'accesso ai dati a livello del record. Le autorizzazioni "Visualizza tutto" e "Modifica tutto" sovrascrivono le impostazioni di condivisione per oggetti specifici. Inoltre le autorizzazioni "Visualizza tutti i dati" e "Modifica tutti i dati" sovrascrivono le impostazioni di condivisione per *tutti* gli oggetti.

La seguente tabella descrive le differenze tra i modelli di protezione.

| | Autorizzazioni che rispettano la condivisione | Autorizzazioni che ignorano la condivisione |
|---|---|---|
| **Destinatari** | Utenti finali | Amministratori dati delegati |
| **Dove gestiti** | Autorizzazioni oggetto "Lettura", "Crea", "Modifica" ed "Elimina";<br>Impostazioni di condivisione | "Visualizza tutto" e "Modifica tutto" |
| **Livelli di accesso ai record** | Privato, Sola lettura, Lettura/Scrittura, Lettura/Scrittura/Trasferimento/Accesso completo | "Visualizza tutto" e "Modifica tutto" |
| **Possibilità di trasferire** | Rispetta le impostazioni di condivisione che variano in base all'oggetto | Disponibile su tutti gli oggetti con autorizzazione "Modifica tutto" |
| **Possibilità di approvare i record o di modificare e sbloccare i record in un processo di approvazione** | Nessuno | Disponibile su tutti gli oggetti con autorizzazione "Modifica tutto" |
| **Possibilità di creare rapporti su tutti i record** | Disponibile con una regola di condivisione che afferma: i record di cui è titolare il gruppo pubblico "Intera organizzazione" | Disponibile su tutti gli oggetti con autorizzazione "Visualizza tutto" |

| | Autorizzazioni che rispettano la condivisione | Autorizzazioni che ignorano la condivisione |
|---|---|---|
| | sono condivisi con un gruppo specifico che dispone dell'accesso Sola lettura | |
| **Supporto degli oggetti** | Disponibile su tutti gli oggetti ad eccezione di prodotti, documenti, soluzioni, idee, note e allegati | Disponibile nella maggior parte degli oggetti tramite le autorizzazioni oggetto<br>Nota: "Visualizza tutto" e "Modifica tutto" non sono disponibili per idee, listini prezzi, tipi di articoli e prodotti. |
| **Livelli di accesso gruppi determinati da** | Ruoli, Ruoli e subordinati, Ruoli e subordinati interni, Ruoli, Subordinati interni e portale, Aree di attesa, Team e Gruppi pubblici | Profilo o insiemi di autorizzazioni |
| **Accesso record privato** | Non disponibile | Disponibile su referenti, opportunità e note e allegati privati con “Visualizza tutto” e “Modifica tutto” |
| **Possibilità di condividere manualmente i record** | Disponibile al titolare del record e a qualsiasi utente con posizione superiore al titolare del record nella gerarchia dei ruoli | Disponibile su tutti gli oggetti con autorizzazione “Modifica tutto” |
| **Capacità di gestire tutti i commenti sui casi** | Non disponibile | Disponibile su tutti i casi con autorizzazione “Modifica tutto” |

## Autorizzazioni sui campi

Le autorizzazioni sui campi specificano il livello di accesso per i singoli campi di un oggetto. Negli insiemi di autorizzazioni e nell'interfaccia utente profilo ottimizzata, le etichette delle impostazioni sono diverse rispetto a quelle dell'interfaccia utente profilo originale e delle pagine di protezione a livello di campo per la personalizzazione dei campi.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

| Livello di accesso | Impostazioni abilitate negli insiemi di autorizzazioni e nell'interfaccia utente profilo ottimizzata | Impostazioni abilitate nell'interfaccia utente profilo originale e nell'interfaccia di protezione a livello di campo |
|---|---|---|
| Gli utenti possono leggere e modificare il campo. | `Lettura` e `Modifica` | `Visibile` |
| Gli utenti possono leggere il campo ma non modificarlo. | `Lettura` | `Visibile` e `Sola lettura` |

| Livello di accesso | Impostazioni abilitate negli insiemi di autorizzazioni e nell'interfaccia utente profilo ottimizzata | Impostazioni abilitate nell'interfaccia utente profilo originale e nell'interfaccia di protezione a livello di campo |
| --- | --- | --- |
| Gli utenti non possono leggere né modificare il campo. | Nessuno | Nessuno |

VEDERE ANCHE:

Panoramica sulla protezione a livello di campo

Autorizzazioni sugli oggetti

# Condivisione

## Panoramica sulle impostazioni di condivisione

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

I team non sono disponibili nella versione **Database.com Edition**

In Salesforce è possibile controllare l'accesso ai dati su svariati livelli. Ad esempio, è possibile controllare l'accesso degli utenti agli oggetti con autorizzazioni relative agli oggetti. All'interno degli oggetti, è possibile controllare l'accesso degli utenti ai campi mediante la protezione a livello di campo. Per controllare l'accesso ai dati a livello di record, utilizzare le impostazioni di condivisione.

### Impostazioni predefinite organizzazione

Le impostazioni di condivisione predefinite dell'organizzazione forniscono un livello di accesso di base a ciascun oggetto e consentono di estendere tale livello di accesso mediante le gerarchie o le regole di condivisione. Ad esempio, è possibile impostare il valore predefinito dell'organizzazione per i lead su Privato se si desidera che gli utenti possano visualizzare e modificare soltanto i lead di cui sono titolari. Quindi, è possibile creare le regole di condivisione dei lead in modo da estendere l'accesso ai lead a utenti o gruppi specifici.

### Regole di condivisione

Le regole di condivisione rappresentano le eccezioni alle impostazioni predefinite dell'organizzazione. Se le impostazioni predefinite di condivisione dell'organizzazione sono Sola lettura pubblica o Privato, è possibile definire regole che forniscano a più utenti l'accesso ai record di cui non sono titolari. È possibile creare le regole di condivisione in base al titolare del record o ai valori dei campi nel record.

Suggerimento: Talvolta non è possibile definire un gruppo omogeneo di utenti che necessitano di accesso a un particolare insieme di record. In tali situazioni, i titolari di record possono utilizzare la condivisione manuale per concedere le autorizzazioni di lettura e modifica agli utenti che altrimenti non avrebbero accesso al record in alcun modo. Benché non sia automatica come le impostazioni di condivisione dell'organizzazione, le gerarchie dei ruoli o le regole di condivisione, la condivisione manuale consente ai titolari dei record di condividere determinati record con gli utenti che ne hanno l'esigenza.

### Condivisione gestita Apex

La condivisione gestita Apex consente agli sviluppatori di condividere gli oggetti personalizzati a livello di programmazione. Quando si utilizza la condivisione gestita Apex per condividere un oggetto personalizzato, solo gli utenti che dispongono dell'autorizzazione

"Modifica tutti i dati" possono aggiungere o cambiare la condivisione sul record dell'oggetto personalizzato e l'accesso in condivisione viene mantenuto per i cambiamenti apportati dal titolare del record.

## Altri metodi per consentire l'accesso ai record

Oltre alle impostazioni di condivisione, esistono altri metodi per consentire a più utenti di accedere a determinati record.

**Mappare i gruppi di categorie ai ruoli**

Controllare l'accesso alle categorie di dati mappandole ai ruoli utente.

**Aree di attesa**

Le aree di attesa consentono ai team di gestire con più facilità i lead, gli ordini, i casi, i contratti di servizio e gli oggetti personalizzati. Dopo che i record sono stati posizionati in un'area di attesa manualmente o mediante regole di assegnazione di lead e casi automatiche, essi rimangono nell'area di attesa finché non vengono assegnati a un utente o presi da uno dei membri dell'area di attesa. Tutti i membri dell'area di attesa e gli utenti al di sopra di loro nella gerarchia dei ruoli possono diventare titolari dei record di un'area di attesa. Utilizzare le aree di attesa per inoltrare record di lead, ordini, casi e oggetti personalizzati a un gruppo.

**Team**

Per gli account, le opportunità e i casi, i titolari dei record possono utilizzare i team per consentire ad altri utenti di accedere ai loro record. Un *team* è un gruppo di utenti che lavorano insieme su un account, sulle opportunità di vendita o su un caso. I titolari dei record possono creare un team per ogni record di cui sono titolari. Il titolare dei record aggiunge i membri del team e per ogni membro del team specifica il livello di accesso al record; pertanto, alcuni membri del team possono avere un accesso di sola lettura e altri un accesso in lettura/scrittura. Il titolare del record può anche specificare un ruolo per ogni membro del team, ad esempio "Sponsor responsabile". Nei team account, i membri del team hanno accesso anche ai referenti, alle opportunità e ai casi associati a un account.

Nota: un membro del team può disporre di un livello di accesso a un record superiore per altri motivi, ad esempio un ruolo o una regola di condivisione. In tal caso, il membro del team ha il livello massimo di accesso concesso, indipendentemente dal livello di accesso specificato nel team.

VEDERE ANCHE:

Informazioni sui valori predefiniti di condivisione dell'organizzazione

Panoramica sulle regole di condivisione

Ruoli

Considerazioni sulla condivisione

## Informazioni sui valori predefiniti di condivisione dell'organizzazione

Gli amministratori possono utilizzare le impostazioni di condivisione a livello dell'organizzazione per definire le impostazioni di condivisione predefinite di un'organizzazione. Le impostazioni di condivisione dell'organizzazione specificano il livello predefinito di accesso ai record e possono essere impostate separatamente per account (compresi i contratti), attività, asset, referenti, campagne, casi, lead, opportunità, calendari, listini prezzi, ordini e oggetti personalizzati.

Per la maggior parte degli oggetti, tali impostazioni di condivisione possono essere impostate su Privato, Sola lettura pubblica o Lettura/Scrittura pubblica. Negli ambienti in cui l'impostazione di condivisione dell'organizzazione per un oggetto è Privato o Solo lettura pubblica, un amministratore può concedere agli utenti livelli di accesso aggiuntivi ai record impostando una gerarchia dei ruoli o definendo regole di condivisione. Tuttavia, le regole di condivisione possono essere utilizzate solo per concedere livelli di accesso aggiuntivi e non per limitare l'accesso ai record oltre quanto previsto originariamente mediante le impostazioni di condivisione predefinite dell'organizzazione.

Importante: se l'organizzazione utilizza un Portale Clienti, prima di abilitare i referenti per l'accesso al portale, impostare i valori predefiniti di condivisione dell'organizzazione relativi ad account, referenti, contratti, asset e casi su Privato. In questo modo, per impostazione predefinita, i clienti potranno visualizzare solo i propri dati. È possibile comunque garantire agli utenti Salesforce l'accesso in Lettura/Scrittura pubblica creando regole di condivisione in cui tutti gli utenti interni possono condividere i dati tra loro.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**.

Il Portale Clienti non è disponibile nella versione **Database.com Edition**

Per impostazione predefinita Salesforce utilizza le gerarchie, quali la gerarchia dei ruoli o dei territori, per concedere automaticamente l'accesso ai record agli utenti che sono in una posizione superiore rispetto al titolare del record nella gerarchia.

Se si imposta un oggetto su Privato, i record sono visibili solo ai titolari e agli utenti di grado superiore nella gerarchia dei ruoli. Utilizzare la casella di controllo **Concedi accesso tramite le gerarchie** per disabilitare l'accesso ai record per gli utenti che sono in una posizione superiore a quella del titolare del record nella gerarchia per gli oggetti personalizzati nelle versioni Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition e Developer Edition. Se si deseleziona questa casella di controllo per un oggetto personalizzato, solo il titolare del record e gli utenti a cui l'accesso è stato garantito dai valori predefiniti a livello di organizzazione potranno accedere ai record.

VEDERE ANCHE:

Impostazione dei valori predefiniti di condivisione della propria organizzazione

Impostazioni predefinite di accesso in condivisione

Impostazioni di condivisione predefinite dell'organizzazione

## Impostazione dei valori predefiniti di condivisione della propria organizzazione

Le impostazioni predefinite di condivisione a livello dell'organizzazione definiscono l'accesso di base per i record. È possibile impostare separatamente le opzioni predefinite per diversi oggetti.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per impostare l'accesso in condivisione predefinito:

- "Gestisci condivisione"

1. Da Imposta, immettere *Impostazioni di condivisione* nella casella Ricerca veloce, quindi selezionare **Impostazioni di condivisione**.
2. Fare clic su **Modifica** nella sezione Impostazioni predefinite organizzazione.
3. Per ogni oggetto, selezionare l'accesso predefinito da utilizzare. Se si dispone di impostazioni predefinite esterne a livello di tutta l'organizzazione, vederePanoramica sulle impostazioni predefinite esterne dell'organizzazione.
4. Per disabilitare l'accesso automatico mediante le gerarchie, deselezionare **Concedi accesso tramite le gerarchie** per qualsiasi oggetto personalizzato che non ha un accesso predefinito di Controllato da società controllante.

   Nota: se la casella di controllo **Concedi accesso tramite le gerarchie** non è selezionata, gli utenti che occupano posizioni superiori nella gerarchia dei ruoli o dei territori non ricevono il diritto di accesso automatico. Tuttavia alcuni utenti, ad esempio quelli che dispongono delle autorizzazioni a livello di oggetto "Visualizza tutto" e "Modifica tutto" e delle autorizzazioni di sistema "Visualizza tutti i dati" e "Modifica tutti i dati", possono comunque accedere ai record di cui non sono titolari.

Quando si aggiornano le impostazioni predefinite dell'organizzazione, il ricalcolo della condivisione applica le modifiche di accesso ai record. Se i dati sono numerosi, l'aggiornamento può durare più a lungo.

- Se si sta innalzando l'accesso predefinito, ad esempio da Solo lettura pubblica a Lettura/Scrittura pubblica, le modifiche hanno effetto immediato. Tutti gli utenti ottengono l'accesso in base all'accesso predefinito aggiornato. Il ricalcolo condivisione viene quindi eseguito in modo asincrono per assicurare l'eliminazione di tutti gli accessi ridondanti provenienti dalle regole manuali o di condivisione.

  Nota: quando l'accesso predefinito per i referenti è Controllato da società controllante e si innalza l'accesso predefinito per account, opportunità o casi, le modifiche hanno effetto dopo l'esecuzione del ricalcolo.

- Se si sta riducendo l'accesso predefinito, ad esempio da Lettura/Scrittura pubblica a Solo lettura pubblica, le modifiche hanno effetto dopo l'esecuzione del ricalcolo.

Quando il ricalcolo è completo, si riceverà una notifica tramite email. Aggiornare la pagina Impostazioni di condivisione per visualizzare le modifiche. Per visualizzare lo stato dell'aggiornamento, da Imposta, immettere *Visualizza itinerario di controllo impostazioni* nella casella Ricerca veloce, quindi selezionare **Visualizza itinerario di controllo impostazioni**.

### Limiti

Per alcuni oggetti non è possibile modificare le impostazioni di condivisione predefinite dell'organizzazione:

- I contratti di servizio sono sempre impostati su Privato.
- Le richieste di provisioning dell'utente sono sempre Private.
- La capacità di visualizzare o modificare un documento, un rapporto o un cruscotto digitale si basa sull'accesso dell'utente alla cartella in cui è memorizzato.
- Un utente può visualizzare solo le previsioni di altri utenti che si trovano a un livello inferiore nella gerarchia dei ruoli, a meno che non sia stata abilitata la condivisione delle previsioni.
- se un oggetto personalizzato è il record dettaglio in una relazione record principale-record dettaglio con un oggetto standard, la relativa impostazione predefinita di tutta l'organizzazione è Controllato da società controllante e non è modificabile.

- Non è possibile trasformare da private a pubbliche le impostazioni predefinite a livello di organizzazione per un oggetto personalizzato se Apex code utilizza le voci di condivisione associate a tale oggetto. Ad esempio, se Apex code recupera gli utenti e i gruppi che accedono in condivisione a un oggetto personalizzato Invoice__c (rappresentato come `Invoice__share` nel codice), non è possibile trasformare da privata a pubblica l'impostazione di condivisione dell'oggetto valida per tutta l'organizzazione.

VEDERE ANCHE:

Impostazioni predefinite di accesso in condivisione

Informazioni sui valori predefiniti di condivisione dell'organizzazione

## Impostazioni predefinite di accesso in condivisione

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Nella versione **Database.com** Edition sono disponibili solo gli oggetti personalizzati.

AUTORIZZAZIONI UTENTE

Per impostare l'accesso in condivisione predefinito:

- "Gestisci condivisione"

È possibile utilizzare le impostazioni predefinite di tutta l'organizzazione per impostare il livello predefinito dell'accesso al record per i seguenti oggetti.

- Account e i contratti associati
- Attività
- Calendari
- Campagne
- Casi
- Referenti
- Oggetti personalizzati
- Lead
- Opportunità
- Ordini
- Listini prezzi
- Contratti di servizio
- Utenti

È possibile assegnare i seguenti livelli di accesso ad account, campagne, casi, referenti, contratti, lead, opportunità, ordini, utenti e oggetti personalizzati.

| Campo | Descrizione |
| --- | --- |
| `Controllato da società controllante` | Un utente può eseguire un'azione su un referente o su un ordine (ad esempio visualizzare, modificare o eliminare) se è in grado di eseguire la stessa azione sul record associato a tale referente.<br><br>Ad esempio se un referente è associato all'account Acme, l'utente può modificare quel referente solo se può modificare anche l'account Acme. |
| `Privato` | Solo il titolare del record e gli utenti con un ruolo superiore nella gerarchia dei ruoli possono visualizzare, modificare e generare rapporti su tali record. |

| Campo | Descrizione |
|---|---|
| | Ad esempio, se Giacomo è il titolare di un account e gli viene assegnato il ruolo di Addetto Vendite Area Ovest con riporto diretto a Carlo, che ricopre il ruolo di Direttore Vendite Area Ovest, anche Carlo potrà visualizzare, modificare e generare rapporti sugli account di Giacomo. |
| `Sola lettura pubblica` | Tutti gli utenti possono visualizzare e generare rapporti sui record, ma non possono modificarli. Solo il titolare e gli utenti con un ruolo superiore nella gerarchia dei ruoli possono modificare tali record.<br>Ad esempio, Sara è il titolare dell'account ABC Spa. Sara ricopre il ruolo di Addetto Vendite Area Ovest, con riporto diretto a Carla, che ricopre il ruolo di Direttore Vendite Area Ovest. Sara e Carla avranno accesso in lettura e scrittura all'account ABC Spa, mentre Giacomo, altro Addetto Vendite Area Ovest, potrà visualizzare e creare rapporti su ABC Spa, ma non potrà modificare l'account. |
| `Lettura/Scrittura pubblica` | Tutti gli utenti possono visualizzare, modificare e generare rapporti su tutti i record.<br>Ad esempio, se Giacomo è il titolare del record Trident Srl, tutti gli utenti potranno visualizzare, modificare e generare rapporti sull'account Trident Srl. Tuttavia, solo Giacomo potrà modificare le impostazioni di condivisione o eliminare l'account Trident. |
| `Lettura/Scrittura/Trasferimento pubblico` | Tutti gli utenti possono visualizzare, modificare, trasferire e generare rapporti su tutti i record. Questa opzione è disponibile solo per i casi e i lead.<br>Ad esempio, se Alice è la titolare del caso ACM numero 100, tutti gli altri utenti potranno visualizzare, modificare, trasferire la proprietà e generare rapporti sul caso. Tuttavia, solo Alice potrà eliminare o modificare la condivisione del caso 100. |
| `Accesso completo pubblico` | Tutti gli utenti possono visualizzare, modificare, trasferire, eliminare e generare rapporti su tutti i record. Disponibile solo per le campagne.<br>Ad esempio, se Marco è il titolare di una campagna, tutti gli altri utenti possono visualizzare, modificare, trasferire o eliminare tale campagna. |

Nota: per utilizzare efficacemente i casi, impostare il valore predefinito per tutta l'organizzazione su Lettura/Scrittura pubblica per Account, Referenti, Contratti e Asset.

È possibile specificare i seguenti livelli di accesso ai calendari personali.

| Campo | Descrizione |
|---|---|
| `Nascondi dettagli` | Altri utenti possono visualizzare la disponibilità dell'utente, tuttavia non possono visualizzare eventuali altre informazioni sulla natura degli eventi inclusi nel calendario dell'utente. |
| `Nascondi dettagli e Aggiungi eventi` | Oltre ai livelli di condivisione impostati dall'opzione Nascondi dettagli, gli utenti possono inserire eventi nei calendari di altri utenti. |
| `Mostra dettagli` | Gli utenti possono visualizzare le informazioni dettagliate relative agli eventi inclusi nei calendari di altri utenti. |
| `Mostra dettagli e Aggiungi eventi` | Oltre ai livelli di condivisione impostati dall'opzione Mostra dettagli, gli utenti possono inserire eventi nei calendari di altri utenti. |
| `Accesso completo` | Gli utenti possono visualizzare le informazioni dettagliate relative agli eventi inclusi nei calendari di altri utenti, nonché inserire eventi e modificare eventi esistenti. |

Nota: indipendentemente dalle impostazioni predefinite di tutta l'organizzazione impostate per i calendari, tutti gli utenti possono invitare tutti gli altri utenti agli eventi.

È possibile specificare i seguenti livelli di accesso ai listini prezzi.

| Campo | Descrizione |
|---|---|
| `Usa` | Tutti gli utenti possono visualizzare i listini prezzi e aggiungervi opportunità. Gli utenti possono aggiungere a un'opportunità qualsiasi prodotto incluso in tale listino prezzi. |
| `Solo visualizzazione` | Tutti gli utenti possono visualizzare e generare rapporti sui listini prezzi, ma solo gli utenti che dispongono dell'autorizzazione "Modifica" per le opportunità o gli utenti ai quali è stato concesso manualmente l'accesso Utilizzo al listino prezzi possono aggiungerli alle opportunità. |
| `Nessun accesso` | Gli utenti non possono visualizzare i listini prezzi né aggiungerli alle opportunità. Utilizzare questo livello di accesso come impostazione predefinita a livello di organizzazione se si desidera che solo determinati utenti possano accedere a listini prezzi specifici. Condividere quindi manualmente i listini prezzi desiderati con gli utenti appropriati. |

È possibile specificare i seguenti livelli di accesso alle attività.

| Campo | Descrizione |
|---|---|
| `Privato` | Solo il titolare dell'attività, e gli utenti con una posizione più alta rispetto al titolare delle attività nella gerarchia dei ruoli, possono modificare ed eliminare l'attività. Gli utenti con accesso in lettura |

| Campo | Descrizione |
| --- | --- |
| | al record a cui è associata l'attività possono visualizzare e creare un rapporto sull'attività. |
| `Controllato da società controllante` | Un utente può eseguire un'azione su un'attività (ad esempio visualizzare, modificare, trasferire o eliminare) se è in grado di eseguire la stessa azione sui record associati a tale attività.<br>Ad esempio se un'operazione è associata all'account Acme e al referente Mario Rossi, l'utente può modificare quell'operazione solo se può modificare anche l'account Acme e il record Mario Rossi. |

È possibile assegnare i seguenti livelli di accesso agli utenti.

| Campo | Descrizione |
| --- | --- |
| `Privato` | Tutti gli utenti hanno accesso in lettura ai loro record utente e ai loro subordinati nella gerarchia dei ruoli. |
| `Sola lettura pubblica` | Tutti gli utenti hanno accesso in lettura reciproco. È possibile visualizzare le pagine dei dettagli di tutti gli utenti. È possibile anche vedere tutti gli utenti nelle ricerche, nelle visualizzazioni elenco, nella variazioni di proprietà e nelle operazioni degli utenti. |

VEDERE ANCHE:

Impostazione dei valori predefiniti di condivisione della propria organizzazione

## Impostazioni di condivisione predefinite dell'organizzazione

Le impostazioni di condivisione predefinite valide per tutta l'organizzazione sono:

| Oggetto | Accesso predefinito |
|---|---|
| Account | Lettura/Scrittura pubblica |
| Attività | Privato |
| Asset | Controllato da società controllante |
| Calendario | Nascondi dettagli e Aggiungi eventi |
| Campagna | Accesso completo pubblico |
| Caso | Lettura/Scrittura/Trasferimento pubblico |
| Referente | Controllato da società controllante |
| Contratto | Lettura/Scrittura pubblica |
| Oggetto personalizzato | Lettura/Scrittura pubblica |
| Lead | Lettura/Scrittura/Trasferimento pubblico |
| Opportunità | Sola lettura pubblica |
| Listino prezzi | Usa |
| Contratto di servizio | Privato |
| Utenti | Sola lettura pubblica<br>Privato per gli utenti esterni |

EDIZIONI

Account, casi, referenti, lead, opportunità e oggetti personalizzati disponibili in: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**.

Nella versione **Database.com Edition** non sono disponibili tutti i tipi di oggetti, fatta eccezione per gli oggetti personalizzati.

VEDERE ANCHE:

Informazioni sui valori predefiniti di condivisione dell'organizzazione

Impostazione dei valori predefiniti di condivisione della propria organizzazione

## Panoramica sulle impostazioni predefinite esterne dell'organizzazione

Le impostazioni predefinite esterne dell'organizzazione prevedono impostazioni predefinite separate a livello di organizzazione per gli utenti interni ed esterni. Semplificano la configurazione delle regole di condivisione e migliorano le prestazioni del ricalcolo. Inoltre, gli amministratori possono vedere facilmente le informazioni condivise con i portali e con altri utenti esterni.

I seguenti oggetti supportano le impostazioni predefinite esterne dell'organizzazione.

- Account e contratti e asset associati.
- Casi
- Referenti
- Opportunità
- Oggetti personalizzati
- Utenti

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Gli utenti esterni includono:

- utenti di siti Web autenticati
- utenti Chatter esterni
- utenti delle comunità
- utenti del Portale Clienti
- utenti guest
- utenti del portale a volume elevato
- utenti del portale partner
- utenti del portale Service Cloud

Nota: Gli utenti esterni Chatter possono accedere solo all'oggetto Utente.

In precedenza, se l'organizzazione richiedeva l'accesso Sola lettura pubblica o Lettura/Scrittura pubblica per gli utenti interni ma l'accesso Privato per gli utenti esterni, era necessario impostare l'accesso predefinito su Privato e creare una regola di condivisione per condividere i record con tutti gli utenti interni.

Con le impostazioni predefinite separate dell'organizzazione è possibile ottenere un comportamento simile impostando l'accesso predefinito interno su Sola lettura pubblica o Lettura/Scrittura pubblica e l'accesso predefinito esterno su Privato. Queste impostazioni velocizzano inoltre le prestazioni per rapporti, visualizzazioni elenco, ricerche e query API.

VEDERE ANCHE:

Informazioni sui valori predefiniti di condivisione dell'organizzazione

Definizione delle impostazioni predefinite esterne dell'organizzazione

Impostazioni predefinite di accesso in condivisione

## Definizione delle impostazioni predefinite esterne dell'organizzazione

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per impostare l'accesso in condivisione predefinito:

- "Gestisci condivisione"

Le impostazioni predefinite esterne dell'organizzazione consentono di impostare un livello di accesso predefinito diverso per gli utenti esterni.

Prima di definire le impostazioni predefinite esterne dell'organizzazione, verificare che siano abilitate. Da Imposta, immettere *Impostazioni di condivisione* nella casella `Ricerca veloce`, selezionare **Impostazioni di condivisione** e fare clic sul pulsante **Abilita modello di condivisione esterno**.

Quando si abilitano le impostazioni predefinite esterne a livello dell'organizzazione per la prima volta, l'accesso predefinito interno e l'accesso predefinito esterno sono impostati sul livello di accesso predefinito originale. Ad esempio, se l'impostazione predefinita a livello di organizzazione per i referenti è Privato, anche l'accesso predefinito interno e l'accesso predefinito esterno saranno impostati su Privato.

Per definire l'impostazione predefinita esterna dell'organizzazione per un oggetto:

1. Da Imposta, immettere *Impostazioni di condivisione* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
2. Fare clic su **Modifica** nella sezione Impostazioni predefinite organizzazione.
3. Per ogni oggetto, selezionare l'accesso predefinito da utilizzare.

   È possibile assegnare i seguenti livelli di accesso.

| Livello di accesso | Descrizione |
| --- | --- |
| `Controllato da società controllante` | Gli utenti possono eseguire operazioni (visualizzazione, modifica, eliminazione) su un record che si trova sul lato dettaglio di una relazione record principale-record dettaglio se possono eseguire la stessa operazione su tutti i record principali associati.<br><br>Nota: Per i referenti è necessario impostare `Controllato da società controllante` per l'accesso predefinito sia interno, sia esterno. |
| `Privato` | Solo gli utenti autorizzati ad accedere perché titolari, dotati di autorizzazioni, attraverso la gerarchia dei ruoli, la condivisione manuale o regole di condivisione possono accedere ai record. |
| `Sola lettura pubblica` | Tutti gli utenti possono vedere tutti i record dell'oggetto. |
| `Lettura/Scrittura pubblica` | Tutti gli utenti possono vedere e modificare tutti i record dell'oggetto. |

Nota: L'accesso predefinito esterno deve essere uguale a quello interno o più restrittivo. Ad esempio, è possibile utilizzare un oggetto personalizzato con l'accesso predefinito esterno impostato su Privato e l'accesso predefinito interno impostato su Sola lettura pubblica.

4. Fare clic su **Salva**.

VEDERE ANCHE:

Panoramica sulle impostazioni predefinite esterne dell'organizzazione

## Disabilitazione delle impostazioni predefinite esterne dell'organizzazione

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per disabilitare le impostazioni predefinite esterne dell'organizzazione:
- "Gestisci condivisione"

Quando si disabilitano le impostazioni predefinite esterne dell'organizzazione, il risultato è un'impostazione predefinita a livello di organizzazione per ogni oggetto.

Prima di disabilitare questa funzione, impostare **Accesso predefinito esterno** e **Accesso predefinito interno** sullo stesso livello di accesso per ciascun oggetto.

Per disabilitare le impostazioni predefinite esterne dell'organizzazione:

1. Da Imposta, immettere *`Impostazioni di condivisione`* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
2. Fare clic su **Disabilita modello di condivisione esterno** nella sezione Impostazioni predefinite organizzazione.

Dopo che sono state disabilitate le impostazioni predefinite esterne dell'organizzazione, nell'area delle impostazioni predefinite dell'organizzazione comparirà la voce **Accesso predefinito** al posto delle impostazioni **Accesso predefinito esterno** e **Accesso predefinito interno**. Se sono attive le Condivisioni utente, le impostazioni di **Access predefinito esterno** per gli oggetti account, referente, caso e opportunità rimangono visibili pur essendo disabilitate.

VEDERE ANCHE:

Panoramica sulle impostazioni predefinite esterne dell'organizzazione

# Controllo dell'accesso mediante le gerarchie

Consente di determinare se gli utenti possono accedere ai record di cui non sono titolari, compresi i record per cui l'accesso in condivisione non è attribuito a loro ma a un subordinato nella gerarchia.

Oltre a specificare le impostazioni predefinite di condivisione di tutta l'organizzazione per ciascun oggetto, è possibile indicare se gli utenti hanno accesso ai dati di proprietà di, o condivisi con, utenti subordinati nella gerarchia. Ad esempio, la gerarchia dei ruoli concede automaticamente l'accesso ai record agli utenti che occupano una posizione superiore a quella del titolare del record nella gerarchia. Per impostazione predefinita, l'opzione `Concedi accesso tramite le gerarchie` è abilitata per tutti gli oggetti e può essere modificata solo per gli oggetti personalizzati.

Per controllare l'accesso in condivisione a un oggetto personalizzato mediante le gerarchie, da Imposta immettere *`Impostazioni di condivisione`* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**. Fare clic su **Modifica** nella sezione Impostazioni predefinite organizzazione. Deselezionare `Concedi accesso tramite le gerarchie` se si desidera impedire agli utenti di avere automaticamente accesso ai dati di proprietà di, o condivisi da, loro subordinati nelle gerarchie.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

I territori non sono disponibili nella versione **Database.com Edition**.

AUTORIZZAZIONI UTENTE

Per impostare l'accesso in condivisione predefinito e modificare l'opzione `Concedi accesso tramite le gerarchie`:

- "Gestisci condivisione"

## Note di implementazione

- Indipendentemente dalle impostazioni di condivisione dell'organizzazione, gli utenti possono ottenere accesso ai record di cui non sono titolari mediante altri metodi, quali le autorizzazioni utente come "Visualizza tutti i dati", le regole di condivisione o la condivisione manuale di record individuali.
- L'opzione `Concedi accesso tramite le gerarchie` è sempre selezionata sugli oggetti standard e non è modificabile.
- Se si disabilita l'opzione `Concedi accesso tramite le gerarchie`, la condivisione con un ruolo o un territorio e i subordinati comporta solo la condivisione con gli utenti direttamente associati al ruolo o al territorio selezionati. Gli utenti nei ruoli o territori superiori nelle gerarchie non avranno accesso.
- Se l'organizzazione disabilita l'opzione `Concedi accesso tramite le gerarchie`, le attività associate a un oggetto personalizzato rimangono visibili per gli utenti che si trovano in una posizione superiore a quella dell'assegnatario dell'attività nella gerarchia dei ruoli.
- Se una relazione record principale-record dettaglio viene interrotta con l'eliminazione della relazione, l'impostazione predefinita dell'oggetto personalizzato dettaglio viene ripristinata automaticamente sull'impostazione precedente Lettura/Scrittura pubblica e `Concedi accesso tramite le gerarchie` viene selezionato per impostazione predefinita.
- L'opzione `Concedi accesso tramite le gerarchie` influisce sugli utenti che potranno accedere ai dati quando avviene una condivisione con gruppi pubblici, gruppi personali, aree di attesa, ruoli o territori. Ad esempio, l'opzione **Visualizza tutti gli utenti** visualizza i membri del gruppo e le persone che occupano posizioni superiori nelle gerarchie quando un record è condiviso con loro mediante una regola di condivisione oppure mediante la condivisione manuale ed è stata selezionata l'opzione `Concedi accesso tramite le gerarchie`. Se l'opzione `Concedi accesso tramite le gerarchie` non è selezionata, alcuni utenti di questi gruppi non avranno accesso. L'elenco seguente indica le ragioni-condizioni di accesso che dipendono dall'opzione `Concedi accesso tramite le gerarchie`.

  **Queste ragioni consentono sempre di ottenere l'accesso:**

  Membro gruppo

  Membro area di attesa

  Membro ruolo

Membro ruolo subordinato

Membro territorio

Membro territorio subordinato

**Queste ragioni consentono di ottenere accesso solo tramite le gerarchie:**

Responsabile del membro gruppo

Responsabile del membro area di attesa

Responsabile del ruolo

Responsabile del territorio

Responsabile del ruolo utente del territorio

## Procedure consigliate

- Quando si deseleziona `Concedi accesso tramite le gerarchie`, informare gli utenti in merito ai cambiamenti nei risultati dei rapporti che potranno verificarsi a causa della perdita di visibilità dei dati dei loro subordinati. Ad esempio, se si seleziona "... del team personale" nell'elenco a discesa Visualizza, vengono restituiti i record di proprietà dell'utente. Non saranno inclusi i record di proprietà dei subordinati. Per essere inclusi nella visualizzazione di questo tipo di rapporto, i record dei subordinati devono essere esplicitamente condivisi con l'utente in un altro modo, ad esempio mediante una regola di condivisione o una condivisione manuale. Quindi, se nessun record è stato condiviso manualmente con l'utente, le opzioni "...personali" e "...del team personale" nell'elenco a discesa Visualizza restituiranno gli stessi risultati. Tuttavia, se si sceglie il tipo di rapporto Attività con.... qualsiasi tipo di oggetto personalizzato quando si crea un rapporto personalizzato, verranno restituite le attività assegnate all'utente nonché quelle assegnate ai suoi subordinati nella gerarchia dei ruoli.

VEDERE ANCHE:

Ruoli

# Ruoli

Salesforce offre una gerarchia dei ruoli che è possibile utilizzare unitamente alle impostazioni di condivisione per stabilire i livelli di accesso degli utenti ai dati della propria organizzazione. I ruoli all'interno della gerarchia influiscono sull'accesso a componenti chiave quali record e rapporti.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare, modificare ed eliminare ruoli:
- "Gestisci ruoli"

Per assegnare utenti ai ruoli:
- "Gestisci utenti interni"

Ecco come aprire l'accesso ai record utilizzando la gerarchia dei ruoli se le impostazioni predefinite a livello di tutta l'organizzazione sono più restrittive di Lettura/scrittura pubblica.

Who Sees What: Record Access via the Role Hierarchy

Gli utenti con un determinato livello di ruolo possono visualizzare, modificare ed emettere un rapporto su tutti i dati di cui sono titolari o che condividono con utenti con ruoli sottostanti nella gerarchia, a meno che il modello di condivisione dell'organizzazione per un oggetto stabilisca diversamente. In modo particolare, nell'elenco correlato Impostazioni predefinite organizzazione, è possibile disabilitare l'opzione **Concedi accesso tramite le gerarchie** per un oggetto personalizzato. Quando l'opzione è disabilitata, solo il titolare del record e gli utenti a cui l'accesso è stato garantito dai valori predefiniti a livello di organizzazione potranno accedere ai record dell'oggetto.

Inoltre, i ruoli determinano l'accesso degli utenti a casi, referenti e opportunità indipendentemente da chi sono i titolari di questi record. Il livello di accesso è specificato nella pagina Modifica ruolo. Ad esempio, è possibile impostare l'accesso ai referenti in modo che gli utenti in un determinato ruolo possano modificare tutti i referenti associati agli account di cui sono titolari, indipendentemente da chi sono i titolari dei referenti. Analogamente, è possibile impostare l'accesso alle opportunità in modo che gli utenti in un determinato ruolo possano modificare tutte le opportunità associate agli account di cui sono titolari, indipendentemente da chi sono i titolari delle opportunità.

## Linee guida per un'implementazione efficace dei ruoli

Per implementare i ruoli in modo efficace è necessario capire i comportamenti chiave delle regole e applicare le procedure consigliate.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Per le procedure consigliate su come progettare l'accesso ai record in una grande organizzazione, vedere *Designing Record Access for Enterprise Scale*.

- Per semplificare la gestione degli utenti nelle organizzazioni con un numero elevato di utenti, abilitare amministratori delegati per gestire utenti in ruoli specifici e tutti i ruoli subordinati.
- È possibile creare fino a 500 ruoli per l'organizzazione.
- A ogni utente deve essere assegnato un ruolo, altrimenti i suoi dati non saranno visualizzati nei rapporti opportunità, nei roll-up delle opportunità e in altre visualizzazioni basate sui ruoli.
- Tutti gli utenti che devono avere la facoltà di visualizzare l'intera organizzazione devono appartenere al livello più alto della gerarchia.
- Non è necessario creare singoli ruoli per ogni qualifica nella società. Definire invece una gerarchia dei ruoli per controllare l'accesso alle informazioni inserite dagli utenti nei ruoli di livello inferiore.
- Quando si modifica il ruolo di un utente vengono applicate le regole di condivisione del nuovo ruolo.

- Gli utenti Salesforce Knowledge possono modificare le impostazioni di visibilità della categoria nella pagina dei dettagli del proprio ruolo.
- Per evitare problemi di prestazioni, nessun utente deve essere titolare di più di 10.000 record di un oggetto. Gli utenti che hanno necessità di essere titolari di un numero superiore di oggetti non devono essere assegnati a un ruolo, oppure devono essere collocati in un ruolo separato in cima alla gerarchia. È importante anche mantenere questi utenti al di fuori dei gruppi pubblici che potrebbero essere utilizzati come origine per le regole di condivisione.
- Quando al titolare di un account non è assegnato alcun ruolo, l'accesso in condivisione per i referenti correlati è in Lettura/Scrittura, a condizione che l'impostazione predefinita a livello di organizzazione per i referenti non sia Controllato da società controllante. L'accesso in condivisione sulle opportunità e i casi correlati è Nessun accesso.
- Se l'organizzazione utilizza Gestione territori, le previsioni si basano sulla gerarchia dei territori anziché sulla gerarchia dei ruoli.

## Assegnazione di utenti ai ruoli

È possibile assegnare rapidamente gli utenti a un determinato ruolo.

1. Da Imposta, immettere *Ruoli* nella casella `Ricerca veloce`, quindi selezionare **Ruoli**.
2. Fare clic su **Assegna** accanto al nome del ruolo desiderato.

   Nota: per accedere a questa pagina, è anche possibile fare clic su **Assegna utenti al ruolo** nell'elenco correlato degli utenti del ruolo. Per motivi di efficienza, si consiglia alle organizzazioni di grandi dimensioni di assegnare i ruoli mediante l'API SOAP.

3. Selezionare una voce dall'elenco a discesa per visualizzare gli utenti disponibili.
4. Selezionare un utente sulla sinistra e fare clic su **Aggiungi** per assegnarlo a quel ruolo.

Nota: se si rimuove un utente dall'elenco Utenti selezionati si rimuove l'assegnazione del ruolo per quell'utente.

VEDERE ANCHE:

Ruoli

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per assegnare utenti ai ruoli:

- "Gestisci utenti interni"

## Campi dei ruoli

I campi che compongono una voce di ruolo hanno scopi specifici. Fare riferimento a questa tabella per le descrizioni dei singoli campi e le modalità di funzionamento all'interno di un ruolo.

La visibilità dei campi dipende dalle autorizzazioni e dalle impostazioni di condivisione dell'organizzazione.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per creare o modificare ruoli:

- "Gestisci ruoli"

| Campo | Descrizione |
|---|---|
| `Accesso caso` | Specifica se gli utenti possono accedere ai casi di altri utenti associati agli account di cui gli utenti sono titolari. Questo campo non è visibile se il modello di condivisione dell'organizzazione per i casi è Lettura/Scrittura pubblica. |
| `Accesso referente` | Specifica se gli utenti possono accedere ai referenti di altri utenti associati agli account di cui gli utenti sono titolari. Questo campo non è visibile se il modello di condivisione dell'organizzazione per i referenti è Lettura/Scrittura pubblica oppure Controllata da società controllante. |
| `Etichetta` | Il nome utilizzato per fare riferimento al ruolo o al titolo della posizione nelle pagine dell'interfaccia utente, ad esempio VP vendite zona occidentale. |
| `Modificato da` | Il nome dell'ultimo utente che ha modificato i dettagli di questo ruolo e la data e l'ora di modifica del ruolo. |
| `Accesso opportunità` | Specifica se gli utenti possono accedere alle opportunità di altri utenti associate agli account di cui gli utenti sono titolari. Questo campo non è visibile se il modello di condivisione dell'organizzazione per le opportunità è Lettura/Scrittura pubblica. |
| `Ruolo partner` | Indica se questo ruolo è associato a un account partner. Questo campo è disponibile solo se nell'organizzazione è stato abilitato un Portale Clienti o un portale partner.<br><br>Se questa casella di controllo è selezionata, non è possibile modificare il ruolo. Il numero predefinito di ruoli negli account portale è tre. Il numero dei ruoli si può diminuire o aumentare fino a un massimo di tre. |
| `Nome ruolo` | Il nome univoco utilizzato dall'API e dai pacchetti gestiti. |

| Campo | Descrizione |
|---|---|
| `Nome ruolo come visualizzato sui rapporti` | Un nome del ruolo che appare nei rapporti. Durante la modifica di un ruolo, se il `Nome ruolo` è lungo, è possibile immettere un nome abbreviato in questo campo. |
| `Gruppi di condivisione` | Questi gruppi vengono creati e mantenuti automaticamente. Il gruppo Ruolo contiene tutti gli utenti di questo ruolo più tutti gli utenti dei ruoli superiori. Il gruppo Ruolo e subordinati contiene tutti gli utenti di questo ruolo più tutti gli utenti dei ruoli superiori e inferiori della gerarchia. Il gruppo Ruolo e subordinati interni (disponibile se per l'organizzazione sono abilitati i Portali Clienti o i Portali partner) contiene tutti gli utenti di questo ruolo. Inoltre, contiene tutti gli utenti dei ruoli superiori e inferiori, con l'esclusione degli utenti del Portale Clienti e del Portale partner. |
| `Questo ruolo fa capo a` | Il ruolo superiore a questo nella gerarchia. |

VEDERE ANCHE:

Ruoli

## Definizione di gruppo

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Un gruppo è composto da un insieme di utenti. Un gruppo può contenere singoli utenti, altri gruppi o gli utenti di un determinato ruolo o territorio. Inoltre, può contenere gli utenti di un determinato ruolo o territorio più tutti gli utenti in posizione subordinata a quel ruolo o territorio nella gerarchia.

Esistono due tipi di gruppi:

- **Gruppi pubblici** - Gli amministratori e gli amministratori delegati possono creare i gruppi pubblici. Tutti gli utenti dell'organizzazione possono utilizzare i gruppi pubblici. Ad esempio, un amministratore può creare un gruppo per un programma di carpooling per i dipendenti. Tutti i dipendenti possono quindi utilizzare questo gruppo per condividere record inerenti al programma.
- **Gruppi personali** - Ogni utente può creare gruppi per uso personale. Ad esempio, è possibile che gli utenti debbano assicurarsi che alcuni record vengano sempre condivisi all'interno di un determinato gruppo di lavoro.

È possibile utilizzare i gruppi nei seguenti modi:

- Per impostare l'accesso in condivisione predefinito attraverso una regola di condivisione.
- Per condividere i record con altri utenti.
- Per specificare che si desidera sincronizzare i referenti di cui sono titolari altri utenti.
- Per aggiungere più utenti a una libreria di Salesforce CRM Content.

- Per assegnare agli utenti azioni specifiche in Salesforce Knowledge.

VEDERE ANCHE:

Tipi di membri dei gruppi

Creazione e modifica di gruppi

Visualizzazione degli elenchi di gruppi

Condivisione di record con gruppi di responsabili

Considerazioni sui gruppi pubblici

## Considerazioni sui gruppi pubblici

Per le organizzazioni con molti utenti, tenere presenti questi suggerimenti per ottimizzare le prestazioni quando si creano gruppi pubblici.

- Creare un gruppo quando un minimo di utenti necessita del medesimo tipo di accesso.
- Creare un gruppo per membri che non hanno necessità di entrare o di uscire spesso dai gruppi.
- Evitare di creare gruppi all'interno di gruppi che determinino più di cinque livelli di nidificazione.
- Abilitare l'accesso automatico ai record mediante le gerarchie dei ruoli per i gruppi pubblici selezionando **Concedi accesso tramite le gerarchie** quando si crea un gruppo. Deselezionare invece questa opzione in caso di creazione di un gruppo pubblico con Tutti gli utenti interni come membri.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

VEDERE ANCHE:

Definizione di gruppo

## Tipi di membri dei gruppi

Quando si crea o si modifica un gruppo, è possibile selezionare i seguenti tipi di membri dall'elenco a discesa `Cerca`. A seconda delle impostazioni dell'organizzazione, alcuni tipi potrebbero non essere disponibili.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

I tipi di membri disponibili variano a seconda della versione utilizzata.

AUTORIZZAZIONI UTENTE

Per creare o modificare un gruppo pubblico:

- "Gestisci utenti"

Per creare o modificare il gruppo personale di un altro utente:

- "Gestisci utenti"

| Tipo di membro | Descrizione |
| --- | --- |
| Utenti Portale Clienti | Tutti gli utenti del Portale Clienti. Disponibile solo se per la propria organizzazione è stato abilitato un Portale Clienti. |
| Utenti partner | Tutti i propri utenti partner. Disponibile solo se per la propria organizzazione è stato abilitato un Portale partner. |
| Gruppi personali | Tutti i gruppi personali. Disponibile solo durante la creazione di altri gruppi personali. |
| Ruoli portale | Tutti i ruoli definiti per il Portale partner o il Portale Clienti dell'organizzazione. Sono inclusi tutti gli utenti nel ruolo portale specificato, ad eccezione degli utenti del portale a volume elevato.<br>Nota: Il nome di un ruolo portale include il nome dell'account a cui è associato, ad eccezione degli account personali che, invece, includono l'`Alias` utente. |
| Ruoli portale e subordinati | Tutti i ruoli definiti per il Portale partner o il Portale Clienti dell'organizzazione. Sono inclusi tutti gli utenti nel ruolo portale specificato e tutti gli utenti al di sotto di quel ruolo nella gerarchia dei ruoli del portale, ad eccezione degli utenti del portale a volume elevato.<br>Nota: Il nome di un ruolo portale include il nome dell'account a cui è associato, ad eccezione degli account personali che, invece, includono l'`Alias` utente. |
| Gruppi pubblici | Tutti i gruppi pubblici definiti dall'amministratore. |
| Ruoli | Tutti i ruoli definiti per l'organizzazione. L'aggiunta di un ruolo a un gruppo include tutti gli utenti in quel ruolo, ma non include i ruoli del portale. |

| Tipo di membro | Descrizione |
|---|---|
| Ruoli e subordinati interni | L'aggiunta di un ruolo e dei suoi ruoli subordinati include tutti gli utenti in quel ruolo, nonché tutti gli utenti nei ruoli inferiori a quello. Non sono inclusi i ruoli o gli utenti del portale. |
| Ruoli e subordinati | L'aggiunta di un ruolo e dei suoi ruoli subordinati include tutti gli utenti in quel ruolo, nonché tutti gli utenti nei ruoli inferiori a quello. Disponibile solo se per la propria organizzazione non è stato abilitato alcun portale. |
| Ruoli, subordinati interni e portale | L'aggiunta di un ruolo e dei suoi ruoli subordinati include tutti gli utenti in quel ruolo, nonché tutti gli utenti nei ruoli inferiori a quello. Disponibile solo se per la propria organizzazione è stato abilitato un portale partner o un Portale Clienti. Sono inclusi gli utenti del portale. |
| Utenti | Tutti gli utenti dell'organizzazione Non sono inclusi gli utenti del portale. |

VEDERE ANCHE:

Definizione di gruppo

Condivisione di record con gruppi di responsabili

## Creazione e modifica di gruppi

Solo gli amministratori e gli amministratori delegati possono creare e modificare gruppi pubblici, ma chiunque può creare e modificare il proprio gruppo personale.

Per creare o modificare un gruppo:

1. Fare clic sull'opzione corrispondente al tipo di gruppo:
   - Per i gruppi personali, andare alle impostazioni personali e fare clic sull'opzione che viene visualizzata tra **Informazioni personali** e **Personali**. Quindi, fare clic su **Gruppi personali**. L'elenco correlato Gruppi personali è anche disponibile nella pagina dei dettagli dell'utente.
   - Per i gruppi pubblici, da Imposta immettere *Gruppi pubblici* nella casella Ricerca veloce, quindi selezionare **Gruppi pubblici**.
2. Fare clic su **Nuovo** o su **Modifica** accanto al gruppo che si desidera modificare.
3. Immettere le seguenti informazioni:

| Campo | Descrizione |
|---|---|
| Etichetta | Nome utilizzato per indicare il gruppo nelle pagine dell'interfaccia utente. |
| Nome gruppo (solo per i gruppi pubblici) | Il nome univoco utilizzato dall'API e dai pacchetti gestiti. |

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare o modificare un gruppo pubblico:
- "Gestisci utenti"

Per creare o modificare il gruppo personale di un altro utente:
- "Gestisci utenti"

| | |
|---|---|
| `Concedi accesso tramite le gerarchie` (solo per i gruppi pubblici) | Selezionare **Concedi accesso tramite le gerarchie** per consentire l'accesso automatico ai record in base alle gerarchie di ruolo. Se l'opzione è selezionata, tutti i record condivisi con gli utenti del gruppo vengono condivisi anche con gli utenti di livello superiore nella gerarchia.<br><br>Deselezionare **Concedi accesso tramite le gerarchie** se si crea un gruppo pubblico i cui membri sono tutti utenti interni, per ottimizzare le prestazioni per la condivisione dei record con i gruppi.<br><br>Nota: Se l'opzione **Concedi accesso tramite le gerarchie** è deselezionata, gli utenti che occupano posizioni superiori nella gerarchia dei ruoli non ricevono in diritto di accesso automatico. Tuttavia alcuni utenti, ad esempio quelli che dispongono delle autorizzazioni a livello di oggetto "Visualizza tutto" e "Modifica tutto" e delle autorizzazioni di sistema "Visualizza tutti i dati" e "Modifica tutti i dati", possono comunque accedere ai record di cui non sono titolari. |
| `Ricerca` | Dal menu a discesa `Cerca`, selezionare il tipo di membro da aggiungere. Se il membro che si desidera aggiungere non è visibile, immettere alcune parole chiave nella casella di ricerca e fare clic su **Trova**.<br><br>Nota: per poter vedere i record secondari di proprietà di utenti del portale a volume elevato, i titolari degli account devono essere membri di un gruppo di condivisione del portale autorizzato ad accedere ai dati degli utenti del portale. |
| `Membri selezionati` | Selezionare i membri dalla casella Membri disponibili, quindi fare clic su **Aggiungi** per aggiungerli al gruppo. |
| `Gruppi delegati selezionati` | In questo elenco, specificare i gruppi di amministratori delegati i cui membri possono aggiungere o rimuovere membri da questo gruppo pubblico. Selezionare i gruppi dalla casella Gruppi delegati disponibili e fare clic su **Aggiungi**. Questo elenco appare solo nei gruppi pubblici. |

4. Fare clic su **Salva**.

Nota: quando si modificano gruppi, ruoli e territori, le regole di condivisione vengono ricalcolate automaticamente per aggiungere o rimuovere l'accesso in funzione delle esigenze.

VEDERE ANCHE:

Definizione di gruppo

## Visualizzazione degli elenchi di gruppi

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per modificare un gruppo pubblico:

- "Gestisci utenti"

1. Fare clic sull'opzione corrispondente al tipo di gruppo.
   - Per i gruppi personali, nelle impostazioni personali fare clic su **Informazioni personali** o **Personale**, a seconda dell'opzione visualizzata. Quindi, fare clic su **Gruppi personali**.
   - Per i gruppi pubblici, da Imposta immettere `Gruppi pubblici` nella casella `Ricerca veloce`, quindi selezionare **Gruppi pubblici**.
2. Per visualizzare la pagina dei dettagli di un gruppo, fare clic sul nome del gruppo nell'elenco correlato Gruppi.
   - Per modificare l'appartenenza al gruppo, fare clic su **Modifica**.
   - Per eliminare il gruppo, fare clic su **Elimina**.
   - Per vedere i membri attivi del gruppo, visualizzare l'elenco correlato Membri gruppo.
   - Per visualizzare tutti i membri e gli utenti del gruppo con accesso equivalente perché in posizione superiore nella gerarchia dei ruoli o dei territori, fare clic su **Visualizza tutti gli utenti** per visualizzare l'elenco correlato Tutti gli utenti nel gruppo. Fare clic su **Visualizza membri gruppo** per tornare all'elenco correlato Membri gruppo.

VEDERE ANCHE:

Definizione di gruppo

## Condivisione di record con gruppi di responsabili

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Condividere record in tutta la catena dirigenziale mediante regole di condivisione o condivisione manuale.

La gerarchia dei ruoli controlla il livello di visibilità dei dati per gli utenti dell'organizzazione. Con Spring '15 si possono utilizzare i gruppi di responsabili per condividere i record con la catena dirigenziale anziché con tutti i responsabili nello stesso ruolo in base alla gerarchia dei ruoli. I gruppi di responsabili si possono usare in tutte le circostanze in cui si usano gli altri gruppi, come nelle condivisioni manuali o nelle regole di condivisione. Non si possono tuttavia aggiungere ad altri gruppi e non includono utenti del portale. I gruppi di responsabili possono contenere solo utenti Standard e Chatter Only.

Ogni utente ha due gruppi di responsabili — gruppo di responsabili (1) e gruppo di subordinati del responsabile (2) — dove (1) include i responsabili diretti e indiretti dell'utente e (2) include l'utente e i suoi riporti diretti e indiretti. Nella pagina di impostazione di una regola di condivisione, questi gruppi sono disponibili nell'elenco a discesa Condividi con.

Per capire chi è il responsabile di un utente, da Imposta immettere *Utenti* nella casella `Ricerca veloce`, quindi selezionare **Utenti**. Fare clic sul nome di un utente. Nel campo `Responsabile` nella pagina dei dettagli dell'utente è visualizzato il responsabile dell'utente.

Per consentire agli utenti di condividere record con i gruppi di responsabili, procedere nel modo seguente.

1. Da Imposta, immettere *Impostazioni di condivisione* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
2. Nella pagina Impostazioni di condivisione, fare clic su **Modifica**.
3. In Altre impostazioni, selezionare `Gruppi di responsabili` e fare clic su **Salva**.

Utilizzando i gruppi di responsabili è possibile condividere i record con i gruppi tramite condivisione manuale, regole di condivisione e condivisione gestita Apex. I motivi di condivisione Apex non sono supportati. Per la condivisione gestita Apex, includere l'ID causa, l'ID record e l'ID responsabile gruppo della riga. Per ulteriori informazioni, vedere *Force.com Apex Code Developer's Guide*.

Gli utenti inattivi restano nei gruppi di cui fanno parte, ma tutte le relative regole di condivisione e condivisioni manuali vengono conservate nei gruppi.

Nota: se l'organizzazione ha abilitato le Condivisioni utente, gli utenti a cui non si è autorizzati ad accedere non sono visibili. Inoltre, se chi effettua una query non è autorizzato ad accedere a un altro utente, non può effettuare query neanche nei gruppi di quell'utente.

Esempio: si immagini di avere un oggetto personalizzato per l'analisi delle prestazioni la cui impostazione predefinita a livello di organizzazione è Privato. Dopo che è stata deselezionata la casella di controllo `Concedi accesso tramite le gerarchie`, solo il dipendente titolare del record di analisi lo può visualizzare e modificare. Per condividere le analisi con i vertici della catena dirigenziale, gli amministratori possono creare una regola di condivisione che le condivide con il gruppo di responsabili

di un utente. In alternativa, il dipendente può condividere il record di analisi con il gruppo di responsabili dell'utente mediante condivisione manuale.

VEDERE ANCHE:

Panoramica sulle impostazioni di condivisione
Panoramica sulle regole di condivisione
Categorie di regole di condivisione

## Panoramica sulle regole di condivisione

Consentono di creare eccezioni automatiche alle impostazioni di condivisione dell'organizzazione per insiemi di utenti definiti.

Ad esempio, è possibile utilizzare le regole di condivisione per estendere l'accesso in condivisione agli utenti che fanno parte di gruppi pubblici, ruoli o territori. Le regole di condivisione non possono comunque essere più limitative rispetto alle impostazioni predefinite dell'organizzazione; consentono semplicemente di incrementare l'accesso per determinati utenti.

È possibile creare i seguenti tipi di regole di condivisione.

| Tipo | Basato su | Impostare l'accesso in condivisione predefinito per |
| --- | --- | --- |
| Regole di condivisione account | Titolare del record o altro criterio, inclusi i tipi di record account o i valori di campo | Account e relativi contratti, opportunità, casi ed eventualmente referenti e ordini |
| Regole di condivisione territorio account | Assegnazione territorio | Account e relativi casi, contratti, referenti e opportunità associati |
| Regole di condivisione asset | Titolare dell'asset o altro criterio, inclusi i tipi di record asset o i valori di campo | Singoli record asset |
| Regole di condivisione campagna | Titolare della campagna o altro criterio, inclusi i tipi di record campagna o i valori di campo | Singoli record campagne |
| Regole di condivisione caso | Titolare del caso o altro criterio, inclusi i tipi di record caso o i valori di campo | Singoli casi e account associati |
| Regole di condivisione referente | Titolare del referente o altro criterio, inclusi i tipi di record referente o i valori di campo | Singoli referenti e account associati |
| Regole di condivisione oggetto personalizzato | Titolare dell'oggetto personalizzato o altro criterio, inclusi i tipi di record oggetto | Singoli record di oggetti personalizzati |

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Le regole di condivisione di account, asset e referenti sono disponibili nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Le regole di condivisione territorio account, caso, lead, opportunità, ordine e oggetto personalizzato sono disponibili nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Le regole di condivisione delle campagne sono disponibili nella versione **Professional Edition** con un supplemento di prezzo, e inoltre nelle versioni **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**.

| Tipo | Basato su | Impostare l'accesso in condivisione predefinito per |
|---|---|---|
| | personalizzato o i valori di campo | |
| Regole di condivisione lead | Titolare del lead o altro criterio, inclusi i tipi di record lead o i valori di campo | Singoli lead |
| Regole di condivisione opportunità | Titolare dell'opportunità o altro criterio, inclusi i tipi di record opportunità o i valori di campo | Singole opportunità e account associati |
| Regole di condivisione ordini | Titolare dell'ordine o altro criterio, inclusi i tipi di record ordine o i valori di campo | Singoli ordini |
| Regole di condivisione utente | Appartenenza a gruppi o altri criteri, fra cui il nome utente e se l'utente è attivo | Singoli record utente |
| Regole di condivisione della richiesta di provisioning utente | Solo il titolare della richiesta di provisioning utente; le regole di condivisione basate sui criteri non sono disponibili. | Singoli record di richieste di provisioning utente |

Nota:

- Non è possibile includere gli utenti del portale a volume elevato nelle regole di condivisione poiché questi utenti non dispongono di ruoli e non possono fare parte di gruppi pubblici.
- Per condividere in modo programmatico gli oggetti personalizzati (basati su titolari di record, ma non su altri criteri), gli sviluppatori possono usare Apex. Questo non vale per le condivisioni utente.

VEDERE ANCHE:

Panoramica sulle regole di condivisione basate sui criteri

Considerazioni sulle regole di condivisione

## Panoramica sulle regole di condivisione basate sui criteri

Le regole di condivisione basate sui criteri determinano gli utenti che possono condividere i record con valori basati sui campi. Ad esempio, si supponga di utilizzare un oggetto personalizzato per le domande di impiego, con un campo di elenco di selezione personalizzato denominato "Reparto". È possibile creare una regola di condivisione basata sui criteri che condivide tutte le domande di lavoro nelle quali il campo Reparto è impostato su "IT" con tutti i responsabili IT della propria organizzazione.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Account, opportunità, casi e referenti non sono disponibili nella versione **Database.com Edition**

Nota:

- Sebbene le regole di condivisione basate sui criteri si fondino sui valori presenti nei record e non sui titolari dei record, la gerarchia dei ruoli o dei territori consente comunque agli utenti che occupano le posizioni più elevate nella gerarchia di accedere ai record.
- Non è possibile utilizzare Apex per creare regole di condivisione basate sui criteri. Inoltre, la condivisione basata sui criteri non può essere verificata utilizzando Apex.
- È possibile utilizzare l'API dei metadati per creare regole di condivisione basate sui criteri a partire dall'API versione 24.0.
- Non è possibile includere gli utenti del portale a volume elevato nelle regole di condivisione poiché questi utenti non dispongono di ruoli e non possono fare parte di gruppi pubblici.

È possibile creare regole di condivisione basate sui criteri per account, opportunità, casi, referenti, lead, campagne e oggetti personalizzati. È possibile definire un massimo di 50 regole di condivisione basate sui criteri per oggetto.

- Tipi di record
- Tipi di campo:
  - Numerazione automatica
  - Casella di controllo
  - Data
  - Data/ora
  - Email
  - Numero
  - Percentuale
  - Telefono
  - Elenco di selezione
  - Testo
  - Area di testo
  - URL
  - Relazione di ricerca (con ID utente o ID area di attesa)

Nota: i campi Testo e Area di testo effettuano la distinzione tra maiuscole e minuscole. Ad esempio, una regola di condivisione basata sui criteri che specifica "Responsabile" in un campo di testo non condivide i record con "responsabile" nel campo. Per creare una regola con diversi casi comuni di una parola, immettere ogni valore separato da una virgola.

VEDERE ANCHE:

Panoramica sulle regole di condivisione

## Categorie di regole di condivisione

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Le regole di condivisione di account e referenti sono disponibili nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Le regole di condivisione territorio account, caso, lead e opportunità sono disponibili nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Le regole di condivisione delle campagne sono disponibili nella versione **Professional Edition** con un supplemento di prezzo, e inoltre nelle versioni **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**.

Le regole di condivisione oggetti personalizzati sono disponibili nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**.

I portali Partner e i Portali Clienti sono disponibili in Salesforce Classic.

Durante la definizione di una regola di condivisione, è possibile scegliere tra le seguenti categorie negli elenchi a discesa `di proprietà dei membri di` e `Condividi con`. A seconda del tipo di regola di condivisione e delle funzioni abilitate per l'organizzazione, è possibile che alcune categorie non vengano visualizzate.

> Nota: Non è possibile includere gli utenti del portale a volume elevato nelle regole di condivisione poiché questi utenti non dispongono di ruoli e non possono fare parte di gruppi pubblici.

| Categoria | Descrizione |
| --- | --- |
| Gruppi di responsabili | Tutti i responsabili diretti e indiretti di un utente. |
| Gruppi di subordinati del responsabile | Un responsabile e tutti i riporti diretti e indiretti da lui gestiti. |
| Aree di attesa | Tutti i record di proprietà dell'area di attesa, esclusi quelli di proprietà dei singoli membri dell'area di attesa. Disponibili solo nell'elenco `di proprietà dei membri di`. |
| Gruppi pubblici | Tutti i gruppi pubblici definiti dall'amministratore.<br><br>Se per l'organizzazione è abilitato un Portale partner o un Portale Clienti viene visualizzato il gruppo Tutti gli utenti partner o Tutti gli utenti del Portale Clienti. Questi gruppi includono tutti gli utenti a cui è consentito l'accesso al portale partner o al Portale Clienti, ad eccezione degli utenti del portale a volume elevato. |
| Ruoli | Tutti i ruoli definiti per l'organizzazione, inclusi tutti gli utenti nel ruolo specificato. |
| Ruoli portale | Tutti i ruoli definiti per il Portale partner o il Portale Clienti dell'organizzazione. inclusi tutti gli utenti nel ruolo portale specificato, ad eccezione degli utenti del portale a volume elevato.<br><br>Il nome di un ruolo portale include il nome dell'account a cui è associato, ad eccezione degli account personali che, invece, includono l'`Alias` utente. |
| Ruoli e subordinati | Tutti i ruoli definiti per l'organizzazione, inclusi tutti gli utenti nel ruolo specificato più tutti gli utenti nei ruoli di livello inferiore, tra cui i ruoli del portale partner e del Portale Clienti che contengono gli utenti con un tipo di licenza portale.<br><br>I ruoli portale sono inclusi in questa categoria solo se per l'organizzazione è abilitato un portale partner o un Portale Clienti.<br><br>La categoria di serie di dati Ruoli, subordinati interni e portale è disponibile nell'organizzazione solo dopo che si è creato almeno un ruolo nella gerarchia dei ruoli. |
| Ruoli portale e subordinati | Tutti i ruoli definiti per il Portale partner o il Portale Clienti dell'organizzazione. Sono inclusi tutti gli utenti nel ruolo portale |

| Categoria | Descrizione |
|---|---|
| | specificato e tutti gli utenti al di sotto di quel ruolo nella gerarchia dei ruoli del portale, ad eccezione degli utenti del portale a volume elevato.<br>Il nome di un ruolo portale include il nome dell'account a cui è associato, ad eccezione degli account personali che, invece, includono l'`Alias` utente. |
| Ruoli e subordinati interni | Tutti i ruoli definiti per l'organizzazione, inclusi tutti gli utenti nel ruolo specificato più tutti gli utenti con un ruolo di livello inferiore, esclusi i ruoli del Portale partner e del Portale Clienti.<br>Questa categoria viene visualizzata solo se per l'organizzazione è abilitato un portale partner o un Portale Clienti Salesforce.<br>La categoria di serie di dati Ruoli e subordinati interni è disponibile nell'organizzazione solo dopo aver creato almeno un ruolo nella gerarchia dei ruoli *e* dopo aver abilitato un portale. |
| Ruoli, subordinati interni e portale | Tutti i ruoli definiti per l'organizzazione, inclusi tutti gli utenti nel ruolo specificato più tutti gli utenti con un ruolo di livello inferiore, inclusi i ruoli del portale partner e del Portale Clienti.<br>Questa categoria viene visualizzata solo se per l'organizzazione è abilitato un portale partner o un Portale Clienti Salesforce.<br>La categoria di serie di dati Ruoli e subordinati interni è disponibile nell'organizzazione solo dopo aver creato almeno un ruolo nella gerarchia dei ruoli *e* dopo aver abilitato un portale. |
| Territori | Tutti i territori definiti per l'organizzazione, |
| Territori e subordinati | Tutti i territori definiti per l'organizzazione, incluso il territorio specificato più tutti i territori di livello inferiore. |

VEDERE ANCHE:

Panoramica sulle regole di condivisione

Condivisione di record con gruppi di responsabili

## Creazione di regole di condivisione lead

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare le regole di condivisione:
- "Gestisci condivisione"

Le regole di condivisione lead sono basate sul titolare del record o su un altro criterio, inclusi il tipo di record e alcuni valori di campo. È possibile definire fino a 300 regole di condivisione lead, comprese un massimo di 50 regole di condivisione basate su criteri.

1. Se si prevede di includere gruppi pubblici nella propria regola di condivisione, verificare che siano stati creati i gruppi appropriati.
2. Da Imposta, immettere *Impostazioni di condivisione* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
3. Nell'elenco correlato Regole di condivisione lead, fare clic su **Nuovo**.
4. Immettere **Nome etichetta** e **Nome regola**. L'etichetta è quella della regola di condivisione visualizzata nell'interfaccia utente. Il nome della regola è un nome univoco utilizzato dall'API e dai pacchetti gestiti.
5. Immettere la **Descrizione**. Questo campo descrive la regola di condivisione. È facoltativo e può contenere fino a 1000 caratteri.
6. Selezionare un tipo di regola.
7. A seconda del tipo di regola selezionata, procedere come segue:
   - `Basata sul titolare record`—Nella riga `di proprietà dei membri di`, specificare gli utenti i cui record verranno condivisi: selezionare una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa (o dal campo di ricerca, se la propria organizzazione ha più di 200 aree di attesa, gruppi, ruoli o territori).
   - `Basata sui criteri`—Specificare i criteri Campo, Operatore e Valore che i record devono soddisfare per essere inclusi nella regola di condivisione. I campi disponibili dipendono dall'oggetto selezionato e il valore è sempre un numero o una stringa letterale. Fare clic su **Aggiungi logica dei filtri...** per modificare la relazione predefinita AND tra ciascun filtro.

     Nota: per utilizzare un campo che non è supportato dalle regole di condivisione basate sui criteri, è possibile creare una regola di flusso di lavoro o un trigger Apex per copiare il valore del campo in un campo di testo o numerico e utilizzare quindi quel campo come criterio.
8. Nella riga `Condividi con`, specificare gli utenti che accedono ai dati: selezionare una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa o dal campo di ricerca.
9. Selezionare l'impostazione di accesso in condivisione per gli utenti.

| Impostazione di accesso | Descrizione |
|---|---|
| Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. |
| Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |

10. Fare clic su **Salva**.

VEDERE ANCHE:

Panoramica sulle regole di condivisione

Categorie di regole di condivisione

## Modifica delle regole di condivisione lead

Per le regole di condivisione basate sul titolare, è possibile modificare unicamente le impostazioni di accesso in condivisione. Per le regole di condivisione basate su altri criteri, è possibile modificare i criteri e le impostazioni di accesso in condivisione.

1. Da Imposta, immettere `Impostazioni di condivisione` nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
2. Nell'elenco correlato Regole di condivisione lead, fare clic su **Modifica** accanto alla regola che si desidera modificare.
3. Modificare l'etichetta e il nome della regola, se necessario.
4. Se è stata selezionata una regola basata sul titolare, passare alla fase successiva.

   Se è stata selezionata una regola basata sui criteri, specificare i criteri a cui devono corrispondere i record per essere inclusi nella regola di condivisione. I campi disponibili dipendono dall'oggetto selezionato e il valore deve essere un numero o una stringa letterale. Fare clic su **Aggiungi logica dei filtri...** per modificare la relazione predefinita AND tra ciascun filtro.
5. Selezionare l'impostazione di accesso in condivisione per gli utenti.

| Impostazione di accesso | Descrizione |
| --- | --- |
| Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. |
| Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |

6. Fare clic su **Salva**.

VEDERE ANCHE:

Panoramica sulle regole di condivisione

Categorie di regole di condivisione

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per modificare le regole di condivisione:

- "Gestisci condivisione"

## Creazione di regole di condivisione account

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare le regole di condivisione:

- "Gestisci condivisione"

Le regole di condivisione account possono essere basate sul titolare del record o su altri criteri, tra cui il tipo di record e alcuni valori di campo. È possibile definire fino a 300 regole di condivisione account, incluse un massimo di 50 regole di condivisione basate su criteri.

1. Se si prevede di includere gruppi pubblici nella propria regola di condivisione, verificare che siano stati creati i gruppi appropriati.
2. Da Imposta, immettere *Impostazioni di condivisione* nella casella Ricerca veloce, quindi selezionare **Impostazioni di condivisione**.
3. Nell'elenco correlato Regole di condivisione account, fare clic su **Nuovo**.
4. Immettere **Nome etichetta** e **Nome regola**. L'etichetta è quella della regola di condivisione visualizzata nell'interfaccia utente. Il nome della regola è un nome univoco utilizzato dall'API e dai pacchetti gestiti.
5. Immettere la **Descrizione**. Questo campo descrive la regola di condivisione. È facoltativo e può contenere fino a 1000 caratteri.
6. Selezionare un tipo di regola.
7. A seconda del tipo di regola selezionata, procedere come segue:
   - Basata sul titolare record—Nella riga di proprietà dei membri di, specificare gli utenti i cui record verranno condivisi: selezionare una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa (o dal campo di ricerca, se la propria organizzazione ha più di 200 aree di attesa, gruppi, ruoli o territori).
   - Basata sui criteri—Specificare i criteri Campo, Operatore e Valore che i record devono soddisfare per essere inclusi nella regola di condivisione. I campi disponibili dipendono dall'oggetto selezionato e il valore è sempre un numero o una stringa letterale. Fare clic su **Aggiungi logica dei filtri...** per modificare la relazione predefinita AND tra ciascun filtro.

     Nota: Per utilizzare un campo che non è supportato dalle regole di condivisione basate sui criteri, è possibile creare una regola di flusso di lavoro o un trigger Apex per copiare il valore del campo in un campo di testo o numerico e utilizzare quindi quel campo come criterio.
8. Nella riga Condividi con, specificare gli utenti che accedono ai dati: selezionare una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa o dal campo di ricerca.
9. Selezionare un'impostazione per Accesso asset, contratto e account predefinito.
10. Nei restanti campi, selezionare le impostazioni di accesso per i record associati agli account condivisi.

| Impostazione di accesso | Descrizione |
|---|---|
| Privato<br>(disponibile solo per i referenti, le opportunità e i casi associati) | Gli utenti non possono visualizzare o aggiornare i record, a meno che l'accesso non sia garantito al di fuori di questa regola di condivisione. |
| Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. |
| Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |

Nota: L'opzione `Accesso referente` non è disponibile quando l'impostazione predefinita per i referenti di tutta l'organizzazione è Controllato da società controllante.

11. Fare clic su **Salva**.

VEDERE ANCHE:

Panoramica sulle regole di condivisione
Categorie di regole di condivisione

## Modifica delle regole di condivisione account

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per modificare le regole di condivisione:
- "Gestisci condivisione"

Per le regole di condivisione basate sul titolare, è possibile modificare unicamente le impostazioni di accesso in condivisione. Per le regole di condivisione basate su altri criteri, è possibile modificare i criteri e le impostazioni di accesso in condivisione.

1. Da Imposta, immettere *`Impostazioni di condivisione`* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
2. Nell'elenco correlato Regole di condivisione account, fare clic su **Modifica** accanto alla regola che si desidera modificare.
3. Modificare l'etichetta e il nome della regola, se necessario.
4. Se è stata selezionata una regola basata sul titolare, passare alla fase successiva.

   Se è stata selezionata una regola basata sui criteri, specificare i criteri a cui devono corrispondere i record per essere inclusi nella regola di condivisione. I campi disponibili dipendono dall'oggetto selezionato e il valore deve essere un numero o una stringa letterale. Fare clic su **Aggiungi logica dei filtri...** per modificare la relazione predefinita AND tra ciascun filtro.
5. Selezionare un'impostazione per `Accesso asset, contratto e account predefinito`.
6. Nei restanti campi, selezionare le impostazioni di accesso per i record associati agli account condivisi.

| Impostazione di accesso | Descrizione |
|---|---|
| Privato<br>(disponibile solo per i referenti, le opportunità e i casi associati) | Gli utenti non possono visualizzare o aggiornare i record, a meno che l'accesso non sia garantito al di fuori di questa regola di condivisione. |
| Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. |
| Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |

Nota: L'opzione `Accesso referente` non è disponibile quando l'impostazione predefinita per i referenti di tutta l'organizzazione è Controllato da società controllante.

7. Fare clic su **Salva**.

VEDERE ANCHE:

Panoramica sulle regole di condivisione

Categorie di regole di condivisione

## Creazione di regole di condivisione territorio account

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare le regole di condivisione:

- "Gestisci condivisione"

Le regole di condivisione territorio account sono basate sull'assegnazione dei territori. È possibile definire fino a 300 regole di condivisione territorio account.

1. Se si prevede di includere gruppi pubblici nella propria regola di condivisione, verificare che siano stati creati i gruppi appropriati.
2. Da Imposta, immettere *`Impostazioni di condivisione`* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
3. Nell'elenco correlato Regole di condivisione territorio account, fare clic su **Nuovo**.
4. Immettere **Nome etichetta** e **Nome regola**. L'etichetta è quella della regola di condivisione visualizzata nell'interfaccia utente. Il nome della regola è un nome univoco utilizzato dall'API e dai pacchetti gestiti.
5. Immettere la **Descrizione**. Questo campo descrive la regola di condivisione. È facoltativo e può contenere fino a 1000 caratteri.
6. Nella riga Account in territorio, selezionare Territori o Territori e subordinati dal primo elenco a discesa e un territorio dal secondo elenco a discesa.
7. Nella riga `Condividi con`, specificare gli utenti che accedono ai dati: selezionare una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa o dal campo di ricerca.
8. Selezionare un'impostazione per `Accesso asset, contratto e account predefinito`.
9. Nei restanti campi, selezionare l'impostazione di accesso per i record associati ai territori account condivisi.

| Impostazione di accesso | Descrizione |
| --- | --- |
| Privato<br>(disponibile solo per i referenti, le opportunità e i casi associati) | Gli utenti non possono visualizzare o aggiornare i record, a meno che l'accesso non sia garantito al di fuori di questa regola di condivisione. |
| Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. |
| Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |

**Nota:** L'opzione `Accesso referente` non è disponibile quando l'impostazione predefinita per i referenti di tutta l'organizzazione è Controllato da società controllante.

10. Fare clic su **Salva**.

VEDERE ANCHE:

Panoramica sulle regole di condivisione

Categorie di regole di condivisione

## Modifica delle regole di condivisione territorio account

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per modificare le regole di condivisione:

- "Gestisci condivisione"

Per le regole di condivisione territorio account, è possibile modificare solo le impostazioni di accesso in condivisione e nient'altro.

1. Da Imposta, immettere *`Impostazioni di condivisione`* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
2. Nell'elenco correlato Regole di condivisione territorio account, fare clic su **Modifica** accanto alla regola che si desidera modificare.
3. Modificare l'etichetta e il nome della regola, se necessario.
4. Selezionare l'impostazione di accesso in condivisione per gli utenti.

| Impostazione di accesso | Descrizione |
| --- | --- |
| Privato<br>(disponibile solo per i referenti, le opportunità e i casi associati) | Gli utenti non possono visualizzare o aggiornare i record, a meno che l'accesso non sia garantito al di fuori di questa regola di condivisione. |
| Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. |
| Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |

Nota: L'opzione `Accesso referente` non è disponibile quando l'impostazione predefinita per i referenti di tutta l'organizzazione è Controllato da società controllante.

5. Fare clic su **Salva**.

VEDERE ANCHE:

Panoramica sulle regole di condivisione

Categorie di regole di condivisione

## Creazione di regole di condivisione referente

Le regole di condivisione referente possono essere basate sul titolare del record oppure su altri criteri, tra cui il tipo di record e alcuni valori di campo. È possibile definire fino a 300 regole di condivisione referenti, incluse un massimo di 50 regole di condivisione basate su criteri.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare le regole di condivisione:
- "Gestisci condivisione"

1. Se si prevede di includere gruppi pubblici nella propria regola di condivisione, verificare che siano stati creati i gruppi appropriati.
2. Da Imposta, immettere *`Impostazioni di condivisione`* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
3. Nell'elenco correlato Regole di condivisione referente, fare clic su **Nuovo**.
4. Immettere **Nome etichetta** e **Nome regola**. L'etichetta è quella della regola di condivisione visualizzata nell'interfaccia utente. Il nome della regola è un nome univoco utilizzato dall'API e dai pacchetti gestiti.
5. Immettere la **Descrizione**. Questo campo descrive la regola di condivisione. È facoltativo e può contenere fino a 1000 caratteri.
6. Selezionare un tipo di regola.
7. A seconda del tipo di regola selezionata, procedere come segue:
   - `Basata sul titolare record`—Nella riga `di proprietà dei membri di`, specificare gli utenti i cui record verranno condivisi: selezionare una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa (o dal campo di ricerca, se la propria organizzazione ha più di 200 aree di attesa, gruppi, ruoli o territori).
   - `Basata sui criteri`—Specificare i criteri Campo, Operatore e Valore che i record devono soddisfare per essere inclusi nella regola di condivisione. I campi disponibili dipendono dall'oggetto selezionato e il valore è sempre un numero o una stringa letterale. Fare clic su **Aggiungi logica dei filtri...** per modificare la relazione predefinita AND tra ciascun filtro.

     Nota: per utilizzare un campo che non è supportato dalle regole di condivisione basate sui criteri, è possibile creare una regola di flusso di lavoro o un trigger Apex per copiare il valore del campo in un campo di testo o numerico e utilizzare quindi quel campo come criterio.
8. Nella riga `Condividi con`, specificare gli utenti che accedono ai dati: selezionare una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa o dal campo di ricerca.
9. Selezionare l'impostazione di accesso in condivisione per gli utenti.

| Impostazione di accesso | Descrizione |
|---|---|
| Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. |
| Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |

10. Fare clic su **Salva**.

VEDERE ANCHE:

Panoramica sulle regole di condivisione
Categorie di regole di condivisione

## Modifica delle regole di condivisione referente

Per le regole di condivisione basate sul titolare, è possibile modificare unicamente le impostazioni di accesso in condivisione. Per le regole di condivisione basate su altri criteri, è possibile modificare i criteri e le impostazioni di accesso in condivisione.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per modificare le regole di condivisione:

- "Gestisci condivisione"

1. Da Imposta, immettere *`Impostazioni di condivisione`* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
2. Nell'elenco correlato Regole di condivisione referente, fare clic su **Modifica** accanto alla regola che si desidera modificare.
3. Modificare l'etichetta e il nome della regola, se necessario.
4. Se è stata selezionata una regola basata sul titolare, passare alla fase successiva.

   Se è stata selezionata una regola basata sui criteri, specificare i criteri a cui devono corrispondere i record per essere inclusi nella regola di condivisione. I campi disponibili dipendono dall'oggetto selezionato e il valore deve essere un numero o una stringa letterale. Fare clic su **Aggiungi logica dei filtri...** per modificare la relazione predefinita AND tra ciascun filtro.
5. Selezionare l'impostazione di accesso in condivisione per gli utenti.

| Impostazione di accesso | Descrizione |
|---|---|
| Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. |
| Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |

6. Fare clic su **Salva**.

VEDERE ANCHE:

Panoramica sulle regole di condivisione

Categorie di regole di condivisione

## Creazione di regole di condivisione opportunità

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare le regole di condivisione:
- "Gestisci condivisione"

Le regole di condivisione opportunità possono essere basate sul titolare del record oppure su altri criteri, tra cui il tipo di record e alcuni valori di campo. È possibile definire fino a 300 regole di condivisione opportunità, incluse un massimo di 50 regole di condivisione basate su criteri.

1. Se si prevede di includere gruppi pubblici nella propria regola di condivisione, verificare che siano stati creati i gruppi appropriati.
2. Da Imposta, immettere *Impostazioni di condivisione* nella casella Ricerca veloce, quindi selezionare **Impostazioni di condivisione**.
3. Nell'elenco correlato Regole di condivisione opportunità, fare clic su **Nuovo**.
4. Immettere **Nome etichetta** e **Nome regola**. L'etichetta è quella della regola di condivisione visualizzata nell'interfaccia utente. Il nome della regola è un nome univoco utilizzato dall'API e dai pacchetti gestiti.
5. Immettere la **Descrizione**. Questo campo descrive la regola di condivisione. È facoltativo e può contenere fino a 1000 caratteri.
6. Selezionare un tipo di regola.
7. A seconda del tipo di regola selezionata, procedere come segue:
   - Basata sul titolare record—Nella riga di proprietà dei membri di, specificare gli utenti i cui record verranno condivisi: selezionare una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa (o dal campo di ricerca, se la propria organizzazione ha più di 200 aree di attesa, gruppi, ruoli o territori).
   - Basata sui criteri—Specificare i criteri Campo, Operatore e Valore che i record devono soddisfare per essere inclusi nella regola di condivisione. I campi disponibili dipendono dall'oggetto selezionato e il valore è sempre un numero o una stringa letterale. Fare clic su **Aggiungi logica dei filtri...** per modificare la relazione predefinita AND tra ciascun filtro.

     Nota: per utilizzare un campo che non è supportato dalle regole di condivisione basate sui criteri, è possibile creare una regola di flusso di lavoro o un trigger Apex per copiare il valore del campo in un campo di testo o numerico e utilizzare quindi quel campo come criterio.

8. Nella riga Condividi con, specificare gli utenti che accedono ai dati: selezionare una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa o dal campo di ricerca.
9. Selezionare l'impostazione di accesso in condivisione per gli utenti. Per le regole basate sul titolare o basate sui criteri con proprietà come criteri, il livello Accesso opportunità si applica alle opportunità di proprietà dei membri del gruppo, ruolo o territorio, a prescindere dall'account associato.

| Impostazione di accesso | Descrizione |
|---|---|
| Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. |
| Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |

10. Fare clic su **Salva**.

VEDERE ANCHE:

Panoramica sulle regole di condivisione

Categorie di regole di condivisione

## Modifica delle regole di condivisione opportunità

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per modificare le regole di condivisione:

- "Gestisci condivisione"

Per le regole di condivisione basate sul titolare, è possibile modificare unicamente le impostazioni di accesso in condivisione. Per le regole di condivisione basate su altri criteri, è possibile modificare i criteri e le impostazioni di accesso in condivisione.

1. Da Imposta, immettere `Impostazioni di condivisione` nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
2. Nell'elenco correlato Regole di condivisione opportunità, fare clic su **Modifica** accanto alla regola che si desidera modificare.
3. Modificare l'etichetta e il nome della regola, se necessario.
4. Se è stata selezionata una regola basata sul titolare, passare alla fase successiva.

   Se è stata selezionata una regola basata sui criteri, specificare i criteri a cui devono corrispondere i record per essere inclusi nella regola di condivisione. I campi disponibili dipendono dall'oggetto selezionato e il valore deve essere un numero o una stringa letterale. Fare clic su **Aggiungi logica dei filtri...** per modificare la relazione predefinita AND tra ciascun filtro.
5. Selezionare l'impostazione di accesso in condivisione per gli utenti. Per le regole basate sul titolare o basate sui criteri con proprietà come criteri, il livello `Accesso opportunità` si applica alle opportunità di proprietà dei membri del gruppo, ruolo o territorio, a prescindere dall'account associato.

| Impostazione di accesso | Descrizione |
|---|---|
| Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. |
| Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |

6. Fare clic su **Salva**.

VEDERE ANCHE:

Panoramica sulle regole di condivisione

Categorie di regole di condivisione

## Creazione di regole di condivisione caso

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare le regole di condivisione:
- "Gestisci condivisione"

Le regole di condivisione caso possono essere basate sul titolare del record oppure su altri criteri, tra cui il tipo di record e alcuni valori di campo. È possibile definire fino a 300 regole di condivisione caso, incluse un massimo di 50 regole di condivisione basate su criteri.

1. Se si prevede di includere gruppi pubblici nella propria regola di condivisione, verificare che siano stati creati i gruppi appropriati.
2. Da Imposta, immettere *Impostazioni di condivisione* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
3. Nell'elenco correlato Regole di condivisione caso, fare clic su **Nuovo**.
4. Immettere **Nome etichetta** e **Nome regola**. L'etichetta è quella della regola di condivisione visualizzata nell'interfaccia utente. Il nome della regola è un nome univoco utilizzato dall'API e dai pacchetti gestiti.
5. Immettere la **Descrizione**. Questo campo descrive la regola di condivisione. È facoltativo e può contenere fino a 1000 caratteri.
6. Selezionare un tipo di regola.
7. A seconda del tipo di regola selezionata, procedere come segue:
   - `Basata sul titolare record`—Nella riga `di proprietà dei membri di`, specificare gli utenti i cui record verranno condivisi: selezionare una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa (o dal campo di ricerca, se la propria organizzazione ha più di 200 aree di attesa, gruppi, ruoli o territori).
   - `Basata sui criteri`—Specificare i criteri Campo, Operatore e Valore che i record devono soddisfare per essere inclusi nella regola di condivisione. I campi disponibili dipendono dall'oggetto selezionato e il valore è sempre un numero o una stringa letterale. Fare clic su **Aggiungi logica dei filtri...** per modificare la relazione predefinita AND tra ciascun filtro.

     Nota: per utilizzare un campo che non è supportato dalle regole di condivisione basate sui criteri, è possibile creare una regola di flusso di lavoro o un trigger Apex per copiare il valore del campo in un campo di testo o numerico e utilizzare quindi quel campo come criterio.

8. Nella riga `Condividi con`, specificare gli utenti che accedono ai dati: selezionare una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa o dal campo di ricerca.
9. Selezionare l'impostazione di accesso in condivisione per gli utenti.

| Impostazione di accesso | Descrizione |
| --- | --- |
| Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. |
| Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |

10. Fare clic su **Salva**.

VEDERE ANCHE:

Panoramica sulle regole di condivisione

Categorie di regole di condivisione

## Modifica delle regole di condivisione caso

Per le regole di condivisione basate sul titolare, è possibile modificare unicamente le impostazioni di accesso in condivisione. Per le regole di condivisione basate su altri criteri, è possibile modificare i criteri e le impostazioni di accesso in condivisione.

1. Da Imposta, immettere *Impostazioni di condivisione* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
2. Nell'elenco correlato Regole di condivisione caso, fare clic su **Modifica** accanto alla regola che si desidera modificare.
3. Modificare l'etichetta e il nome della regola, se necessario.
4. Se è stata selezionata una regola basata sul titolare, passare alla fase successiva.

   Se è stata selezionata una regola basata sui criteri, specificare i criteri a cui devono corrispondere i record per essere inclusi nella regola di condivisione. I campi disponibili dipendono dall'oggetto selezionato e il valore deve essere un numero o una stringa letterale. Fare clic su **Aggiungi logica dei filtri...** per modificare la relazione predefinita AND tra ciascun filtro.
5. Selezionare l'impostazione di accesso in condivisione per gli utenti.

| Impostazione di accesso | Descrizione |
| --- | --- |
| Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. |
| Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |

6. Fare clic su **Salva**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per modificare le regole di condivisione:

- "Gestisci condivisione"

VEDERE ANCHE:

Panoramica sulle regole di condivisione
Categorie di regole di condivisione

## Creazione di regole di condivisione campagna

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition** con un supplemento di prezzo e inoltre nelle versioni **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**.

AUTORIZZAZIONI UTENTE

Per creare le regole di condivisione:

- "Gestisci condivisione"

Le regole di condivisione campagna possono essere basate sul titolare dei record o su un altro criterio, inclusi il tipo di record e alcuni valori di campo. È possibile definire fino a 300 regole di condivisione campagna, comprese un massimo di 50 regole di condivisione basate su criteri.

1. Se si prevede di includere gruppi pubblici nella propria regola di condivisione, verificare che siano stati creati i gruppi appropriati.
2. Da Imposta, immettere *`Impostazioni di condivisione`* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
3. Nell'elenco correlato Regole di condivisione campagna, fare clic su **Nuovo**.
4. Immettere **Nome etichetta** e **Nome regola**. L'etichetta è quella della regola di condivisione visualizzata nell'interfaccia utente. Il nome della regola è un nome univoco utilizzato dall'API e dai pacchetti gestiti.
5. Immettere la **Descrizione**. Questo campo descrive la regola di condivisione. È facoltativo e può contenere fino a 1000 caratteri.
6. Selezionare un tipo di regola.
7. A seconda del tipo di regola selezionata, procedere come segue:
   - `Basata sul titolare record`—Nella riga `di proprietà dei membri di`, specificare gli utenti i cui record verranno condivisi: selezionare una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa (o dal campo di ricerca, se la propria organizzazione ha più di 200 aree di attesa, gruppi, ruoli o territori).
   - `Basata sui criteri`—Specificare i criteri Campo, Operatore e Valore che i record devono soddisfare per essere inclusi nella regola di condivisione. I campi disponibili dipendono dall'oggetto selezionato e il valore è sempre un numero o una stringa letterale. Fare clic su **Aggiungi logica dei filtri...** per modificare la relazione predefinita AND tra ciascun filtro.

     Nota: per utilizzare un campo che non è supportato dalle regole di condivisione basate sui criteri, è possibile creare una regola di flusso di lavoro o un trigger Apex per copiare il valore del campo in un campo di testo o numerico e utilizzare quindi quel campo come criterio.
8. Nella riga `Condividi con`, specificare gli utenti che accedono ai dati: selezionare una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa o dal campo di ricerca.
9. Selezionare l'impostazione di accesso in condivisione per gli utenti.

| Impostazione di accesso | Descrizione |
|---|---|
| Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. |
| Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |
| Accesso completo | Tutti gli utenti di un gruppo, ruolo o territorio selezionato possono visualizzare, modificare, trasferire, eliminare e condividere il record, proprio come il titolare del record.<br><br>Una regola di condivisione di tipo Accesso completo fornisce inoltre agli utenti la possibilità di visualizzare, modificare, eliminare e chiudere le attività associate al record se l'impostazione di condivisione in tutta l'organizzazione per le attività è Controllato da società controllante. |

10. Fare clic su **Salva**.

VEDERE ANCHE:

Panoramica sulle regole di condivisione
Categorie di regole di condivisione

## Modifica delle regole di condivisione campagna

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition** con un supplemento di prezzo e inoltre nelle versioni **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**.

AUTORIZZAZIONI UTENTE

Per modificare le regole di condivisione:
- "Gestisci condivisione"

Per le regole di condivisione basate sul titolare, è possibile modificare unicamente le impostazioni di accesso in condivisione. Per le regole di condivisione basate su altri criteri, è possibile modificare i criteri e le impostazioni di accesso in condivisione.

1. Da Imposta, immettere `Impostazioni di condivisione` nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
2. Nell'elenco correlato Regole di condivisione campagna, fare clic su **Modifica** accanto alla regola che si desidera modificare.
3. Modificare l'etichetta e il nome della regola, se necessario.
4. Se è stata selezionata una regola basata sul titolare, passare alla fase successiva.

   Se è stata selezionata una regola basata sui criteri, specificare i criteri a cui devono corrispondere i record per essere inclusi nella regola di condivisione. I campi disponibili dipendono dall'oggetto selezionato e il valore deve essere un numero o una stringa letterale. Fare clic su **Aggiungi logica dei filtri...** per modificare la relazione predefinita AND tra ciascun filtro.

5. Selezionare l'impostazione di accesso in condivisione per gli utenti.

| Impostazione di accesso | Descrizione |
| --- | --- |
| Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. |
| Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |
| Accesso completo | Tutti gli utenti di un gruppo, ruolo o territorio selezionato possono visualizzare, modificare, trasferire, eliminare e condividere il record, proprio come il titolare del record.<br><br>Una regola di condivisione di tipo Accesso completo fornisce inoltre agli utenti la possibilità di visualizzare, modificare, eliminare e chiudere le attività associate al record se l'impostazione di condivisione in tutta l'organizzazione per le attività è Controllato da società controllante. |

6. Fare clic su **Salva**.

VEDERE ANCHE:

Panoramica sulle regole di condivisione
Categorie di regole di condivisione

## Creazione di regole di condivisione testo veloce

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare le regole di condivisione:

- "Gestisci condivisione"

Per creare le regole di condivisione testo veloce:

1. Se si prevede di includere gruppi pubblici nella propria regola di condivisione, verificare che siano stati creati i gruppi appropriati.
2. Da Imposta, immettere *`Impostazioni di condivisione`* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
3. Nell'elenco correlato delle regole di condivisione testo veloce, fare clic su **Nuovo**.
4. Immettere **Nome etichetta** e **Nome regola**. L'etichetta è quella della regola di condivisione visualizzata nell'interfaccia utente. Il nome della regola è un nome univoco utilizzato dall'API e dai pacchetti gestiti.
5. Immettere la **Descrizione**. Questo campo descrive la regola di condivisione. È facoltativo e può contenere fino a 1000 caratteri.
6. Nella riga `Testo veloce: di proprietà dei membri di`, specificare gli utenti titolari dei dati selezionando una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa.
7. Nella riga `Condividi con`, specificare gli utenti che accedono ai dati: selezionare una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa o dal campo di ricerca.
8. Selezionare l'impostazione di accesso in condivisione per gli utenti.

| Impostazione di accesso | Descrizione |
| --- | --- |
| Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. |
| Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |

9. Fare clic su **Salva**.

VEDERE ANCHE:

Panoramica sulle regole di condivisione

Categorie di regole di condivisione

## Creazione di regole di condivisione oggetto personalizzato

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per creare le regole di condivisione:
- "Gestisci condivisione"

Le regole di condivisione oggetto personalizzato possono essere basate sul titolare del record oppure su altri criteri, tra cui il tipo di record e alcuni valori di campo. È possibile definire fino a 300 regole di condivisione oggetto personalizzato, compreso un massimo di 50 regole di condivisione basate su criteri.

1. Se si prevede di includere gruppi pubblici nella propria regola di condivisione, verificare che siano stati creati i gruppi appropriati.
2. Da Imposta, immettere *`Impostazioni di condivisione`* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
3. Nell'elenco correlato Regole di condivisione dell'oggetto personalizzato, fare clic su **Nuovo**.
4. Immettere l'etichetta e il nome della regola. L'etichetta è quella della regola di condivisione visualizzata nell'interfaccia utente. Il nome della regola è un nome univoco utilizzato dall'API e dai pacchetti gestiti.
5. Immettere la **Descrizione**. Questo campo descrive la regola di condivisione. È facoltativo e può contenere fino a 1000 caratteri.
6. Selezionare un tipo di regola.
7. A seconda del tipo di regola selezionata, procedere come segue:
   - `Basata sul titolare record`—Nella riga `di proprietà dei membri di`, specificare gli utenti i cui record verranno condivisi: selezionare una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa (o dal campo di ricerca, se la propria organizzazione ha più di 200 aree di attesa, gruppi, ruoli o territori).
   - `Basata sui criteri`—Specificare i criteri Campo, Operatore e Valore che i record devono soddisfare per essere inclusi nella regola di condivisione. I campi disponibili dipendono dall'oggetto selezionato e il valore è sempre un numero o una stringa letterale. Fare clic su **Aggiungi logica dei filtri...** per modificare la relazione predefinita AND tra ciascun filtro.

     Nota: per utilizzare un campo che non è supportato dalle regole di condivisione basate sui criteri, è possibile creare una regola di flusso di lavoro o un trigger Apex per copiare il valore del campo in un campo di testo o numerico e utilizzare quindi quel campo come criterio.
8. Nella riga `Condividi con`, specificare gli utenti che accedono ai dati: selezionare una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa o dal campo di ricerca.
9. Selezionare l'impostazione di accesso in condivisione per gli utenti.

| Impostazione di accesso | Descrizione |
|---|---|
| Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. |
| Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |

10. Fare clic su **Salva**.

VEDERE ANCHE:

Panoramica sulle regole di condivisione

Categorie di regole di condivisione

## Modifica delle regole di condivisione oggetto personalizzato

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**.

AUTORIZZAZIONI UTENTE

Per modificare le regole di condivisione:

- "Gestisci condivisione"

Per le regole di condivisione basate sul titolare, è possibile modificare unicamente le impostazioni di accesso in condivisione. Per le regole di condivisione basate su altri criteri, è possibile modificare i criteri e le impostazioni di accesso in condivisione.

1. Da Imposta, immettere *Impostazioni di condivisione* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
2. Nell'elenco correlato Regole di condivisione per l'oggetto personalizzato, fare clic su **Modifica** accanto alla regola che si desidera modificare.
3. Modificare l'etichetta e il nome della regola, se necessario.
4. Se è stata selezionata una regola basata sul titolare, passare alla fase successiva.

   Se è stata selezionata una regola basata sui criteri, specificare i criteri a cui devono corrispondere i record per essere inclusi nella regola di condivisione. I campi disponibili dipendono dall'oggetto selezionato e il valore deve essere un numero o una stringa letterale. Fare clic su **Aggiungi logica dei filtri...** per modificare la relazione predefinita AND tra ciascun filtro.

5. Selezionare l'impostazione di accesso in condivisione per gli utenti.

   | Impostazione di accesso | Descrizione |
   | --- | --- |
   | Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. |
   | Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |

6. Fare clic su **Salva**.

VEDERE ANCHE:

Panoramica sulle regole di condivisione

Categorie di regole di condivisione

## Creazione di regole di condivisione ordini

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare le regole di condivisione:
- "Gestisci condivisione"

Le regole di condivisione ordini possono essere basate sul titolare del record oppure su altri criteri, tra cui il tipo di record e alcuni valori di campo. È possibile definire fino a 300 regole di condivisione ordini, incluse un massimo di 50 regole di condivisione basate su criteri.

1. Se si prevede di includere gruppi pubblici nella propria regola di condivisione, verificare che siano stati creati i gruppi appropriati.
2. Da Imposta, immettere *`Impostazioni di condivisione`* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
3. Nell'elenco correlato Regole di condivisione ordini, fare clic su **Nuovo**.
4. Immettere **Nome etichetta** e **Nome regola**. L'etichetta è quella della regola di condivisione visualizzata nell'interfaccia utente. Il nome della regola è un nome univoco utilizzato dall'API e dai pacchetti gestiti.
5. Immettere la **Descrizione**. Questo campo descrive la regola di condivisione. È facoltativo e può contenere fino a 1000 caratteri.
6. Selezionare un tipo di regola.
7. A seconda del tipo di regola selezionata, procedere come segue:
   - `Basata sul titolare record`—Nella riga `di proprietà dei membri di`, specificare gli utenti i cui record verranno condivisi: selezionare una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa (o dal campo di ricerca, se la propria organizzazione ha più di 200 aree di attesa, gruppi, ruoli o territori).
   - `Basata sui criteri`—Specificare i criteri Campo, Operatore e Valore che i record devono soddisfare per essere inclusi nella regola di condivisione. I campi disponibili dipendono dall'oggetto selezionato e il valore è sempre un numero o una stringa letterale. Fare clic su **Aggiungi logica dei filtri...** per modificare la relazione predefinita AND tra ciascun filtro.

     Nota: per utilizzare un campo che non è supportato dalle regole di condivisione basate sui criteri, è possibile creare una regola di flusso di lavoro o un trigger Apex per copiare il valore del campo in un campo di testo o numerico e utilizzare quindi quel campo come criterio.
8. Nella riga `Condividi con`, specificare gli utenti che accedono ai dati: selezionare una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa o dal campo di ricerca.
9. Selezionare l'impostazione di accesso in condivisione per gli utenti.

| Impostazione di accesso | Descrizione |
| --- | --- |
| Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. |
| Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |

10. Fare clic su **Salva**.

## Modifica delle regole di condivisione ordini

Per le regole di condivisione basate sul titolare, è possibile modificare unicamente le impostazioni di accesso in condivisione. Per le regole di condivisione basate su altri criteri, è possibile modificare i criteri e le impostazioni di accesso in condivisione.

1. Da Imposta, immettere *Impostazioni di condivisione* nella casella Ricerca veloce, quindi selezionare **Impostazioni di condivisione**.
2. Nell'elenco correlato Regole di condivisione ordini, fare clic su **Modifica** accanto alla regola che si desidera modificare.
3. Modificare l'etichetta e il nome della regola, se necessario.
4. Se è stata selezionata una regola basata sul titolare, passare alla fase successiva.

   Se è stata selezionata una regola basata sui criteri, specificare i criteri a cui devono corrispondere i record per essere inclusi nella regola di condivisione. I campi disponibili dipendono dall'oggetto selezionato e il valore deve essere un numero o una stringa letterale. Fare clic su **Aggiungi logica dei filtri...** per modificare la relazione predefinita AND tra ciascun filtro.
5. Selezionare l'impostazione di accesso in condivisione per gli utenti.

| Impostazione di accesso | Descrizione |
| --- | --- |
| Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. |
| Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |

6. Fare clic su **Salva**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per modificare le regole di condivisione:

- "Gestisci condivisione"

## Creazione delle regole di condivisione per le richieste di provisioning utente

Le regole di condivisione delle richieste di provisioning utente possono essere basate esclusivamente sul titolare del record. Non è possibile creare regole di condivisione delle richieste di provisioning utente basate su criteri. È possibile definire fino a 300 regole di condivisione per le richieste di provisioning utente.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare regole di condivisione per le richieste di provisioning utente:

- "Gestisci condivisione" e "Utilizza funzioni Identity"

1. Se si prevede di includere gruppi pubblici nella propria regola di condivisione, verificare che siano stati creati i gruppi appropriati.
2. Da Imposta, immettere *Impostazioni di condivisione* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
3. Nell'elenco correlato delle regole di condivisione per le richieste di provisioning utente, fare clic su **Nuovo**.
4. Immettere **Nome etichetta** e **Nome regola**. L'etichetta è quella della regola di condivisione visualizzata nell'interfaccia utente. Il nome della regola è un nome univoco utilizzato dall'API e dai pacchetti gestiti.
5. Immettere la **Descrizione**. Questo campo descrive la regola di condivisione. È facoltativo e può contenere fino a 1000 caratteri.
6. Nella riga `di proprietà dei membri di`, specificare gli utenti di cui vengono condivisi i record. Selezionare una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa (o dal campo di ricerca, se la propria organizzazione ha più di 200 aree di attesa, gruppi, ruoli o territori).
7. Nella riga `Condividi con`, specificare gli utenti che accedono ai dati: selezionare una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa o dal campo di ricerca.
8. Selezionare l'impostazione di accesso in condivisione per gli utenti.

| Impostazione di accesso | Descrizione |
| --- | --- |
| Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. |
| Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |

9. Fare clic su **Salva**.

VEDERE ANCHE:

Panoramica sulle regole di condivisione

Categorie di regole di condivisione

Modifica delle regole di condivisione per le richieste di provisioning utente

## Modifica delle regole di condivisione per le richieste di provisioning utente

Per le regole di condivisione basate su un titolare, è possibile modificare unicamente le impostazioni di accesso in condivisione. Non è possibile creare regole di condivisione delle richieste di provisioning utente basate su criteri.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per modificare le regole di condivisione:
- "Gestisci condivisione"

1. Da Imposta, immettere `Impostazioni di condivisione` nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
2. Nell'elenco correlato delle regole di condivisione delle richieste di provisioning utente, fare clic su **Modifica** accanto alla regola che si desidera modificare.
3. Modificare l'etichetta e il nome della regola, se necessario.
4. Selezionare l'impostazione di accesso in condivisione per gli utenti.

| Impostazione di accesso | Descrizione |
|---|---|
| Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. |
| Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |

5. Fare clic su **Salva**.

VEDERE ANCHE:

Panoramica sulle regole di condivisione

Categorie di regole di condivisione

## Considerazioni sulle regole di condivisione

Le regole di condivisione permettono di concedere un accesso selettivo ai dati a gruppi di utenti definiti. Prima di utilizzare le regole di condivisione, leggere le note che seguono:

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Le regole di condivisione di account e referenti sono disponibili nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Le regole di condivisione territorio account, caso, lead, opportunità, ordine e oggetto personalizzato sono disponibili nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Le regole di condivisione delle campagne sono disponibili nella versione **Professional Edition** con un supplemento di prezzo, e inoltre nelle versioni **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**.

Nella versione **Database.com** Edition sono disponibili solo le regole di condivisione degli oggetti personalizzati.

**Concessione dell'accesso**

- Le regole di condivisione si possono usare per concedere un accesso più ampio ai dati. L'accesso non si può limitare oltre la soglia stabilita dalle impostazioni predefinite a livello di organizzazione.
- Se più regole di condivisione assegnano a un utente livelli di accesso diversi a un record, l'accesso dell'utente sarà quello più permissivo.
- Le regole di condivisione concedono automaticamente un accesso aggiuntivo ai record correlati. Ad esempio, le regole di condivisione delle opportunità consentono ai ruoli o ai membri dei gruppi di accedere all'account associato all'opportunità condivisa se non sono già autorizzati ad accedervi. Analogamente, le regole di condivisione di referenti e casi consentono ai ruoli o ai membri dei gruppi di accedere anche all'account associato.
- Agli utenti nella gerarchia dei ruoli viene concesso automaticamente il medesimo livello di accesso assegnato da una regola di condivisione agli utenti in posizioni gerarchiche subordinate, a condizione che l'oggetto sia standard o che sia selezionata l'opzione **Concedi accesso tramite le gerarchie**.
- Indipendentemente dalle regole di condivisione, gli utenti possono, come minimo, visualizzare gli account nei propri territori. Inoltre, è possibile concedere agli utenti l'accesso per visualizzare e modificare i referenti, le opportunità e i casi associati agli account dei loro territori.

**Aggiornamento**

- Se si crea una regola di condivisione basata sul titolare con gli stessi gruppi di origine e destinazione di una regola esistente, questa viene sovrascritta.
- Dopo il salvataggio di una regola di condivisione non è possibile modificare le impostazioni del campo `Condividi con` quando si modifica la regola di condivisione.
- Le regole di condivisione sono valide per tutti i record nuovi ed esistenti che soddisfano la definizione della serie di dati di origine.
- Le regole di condivisione valgono sia per gli utenti attivi, sia per quelli inattivi.
- Quando si modificano i livelli di accesso di una regola di condivisione, tutti i record esistenti vengono aggiornati automaticamente con i nuovi livelli di accesso.
- Quando si elimina una regola di condivisione, l'accesso in condivisione creato dalla regola viene automaticamente eliminato.
- Quando si modificano gli utenti all'interno di un gruppo, di un ruolo o di un territorio, le regole di condivisione vengono rivalutate per aggiungere o eliminare l'accesso a seconda dei casi.
- Quando si trasferiscono record da un utente a un altro, le regole di condivisione vengono rivalutate per aggiungere o eliminare l'accesso ai record trasferiti, a seconda dei casi.
- La modifica delle regole di condivisione può richiedere la modifica contemporanea di moltissimi record. Per elaborare le modifiche in modo efficiente, la richiesta potrebbe essere accodata e l'utente potrebbe ricevere un'email di notifica al completamento del processo.
- Le regole di condivisione dei lead non concedono automaticamente l'accesso ai dati dei lead dopo la loro conversione in record account, referente e opportunità.

**Utenti di portali**

- È possibile creare regole per condividere i record fra quasi tutti i tipi di utenti del Portale Clienti e di Salesforce. Analogamente, è possibile creare regole di condivisione fra utenti del Portale Clienti da account diversi, a condizione che dispongano della licenza utente Responsabile Portale Clienti. Non è invece possibile includere gli utenti del portale a volume elevato nelle regole di condivisione poiché questi utenti non dispongono di ruoli e non possono fare parte di gruppi pubblici.
- Utilizzando la Conversione guidata accesso utente portale è possibile convertire facilmente regole di condivisione che includono Ruoli, subordinati interni e portale affinché includano, invece, Ruoli e subordinati interni. Inoltre, la procedura guidata può essere utilizzata per convertire cartelle di rapporti, cruscotti digitali e documenti con accesso pubblico in cartelle accessibili da tutti gli utenti tranne quelli del portale.

**Campi dei pacchetti gestiti**

Se una regola di condivisione basata su criteri fa riferimento a un campo di un pacchetto gestito la cui licenza è scaduta, dopo l'etichetta del campo viene aggiunta la dicitura `(scaduto)`. L'etichetta del campo è visualizzata nell'elenco a discesa dei campi nella pagina di definizione della regola in Imposta. Le regole di condivisione basate su criteri che fanno riferimento a campi scaduti non vengono ricalcolate e i nuovi record non vengono condivisi in base a queste regole. Viene invece conservata la condivisione dei record esistenti già prima della scadenza del pacchetto.

VEDERE ANCHE:

Panoramica sulle regole di condivisione

## Panoramica sulle condivisioni utente

Con la funzione di condivisione standard è possibile controllare quali utenti vede ciascun utente.

Ecco come impostare le condivisioni utente nella propria organizzazione.

Le Condivisioni utente consentono di mostrare o nascondere un utente interno o esterno a un altro utente dell'organizzazione. Ad esempio, si immagini di essere un produttore che deve includere tutti i distributori nella propria organizzazione, ma impedendo loro di vedersi e di interagire. In questo caso è possibile impostare i valori predefiniti a livello di organizzazione per l'oggetto Utente su Privato e quindi estendere l'accesso fra i gruppi di distributori che devono potersi vedere e interagire fra loro nell'organizzazione mediante regole di condivisione o condivisione manuale.

Con le Condivisioni utente è possibile:

- Assegnare l'autorizzazione "Visualizza tutti gli utenti" agli utenti che devono poter vedere tutti gli utenti o interagire con loro. Questa autorizzazione è abilitata automaticamente per gli utenti con l'autorizzazione "Gestisci utenti".
- Impostare l'impostazione predefinita a livello di organizzazione per i record utente su Privato o Sola lettura pubblica.
- Creare regole di condivisione utente basate sull'appartenenza a gruppi o su altri criteri.
- Creare condivisioni manuali per i record utente per estendere l'accesso a singoli utenti o gruppi.
- Controllare la visibilità degli utenti esterni nei Portali Clienti o partner e nelle comunità.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Condivisione manuale, portali e comunità disponibili nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

VEDERE ANCHE:

Condivisioni utente

Ripristino delle impostazioni predefinite di visibilità degli utenti

Controllo degli utenti che possono essere visualizzati dagli utenti dei portali o delle comunità

## Condivisioni utente

Definire le impostazioni predefinite a livello di organizzazione per i record utente interni ed esterni. Estendere poi l'accesso mediante regole di condivisione basate sull'appartenenza a gruppi pubblici, ruoli o territori, oppure condividere manualmente i singoli record utente con altri utenti o gruppi.

Quando si abilitano le condivisioni utente, gli utenti possono vedere gli altri utenti nelle ricerche, nelle visualizzazioni elenco e simili solo se dispongono dell'accesso in Lettura a quegli utenti.

Prima di implementare le condivisioni utente, rivedere le considerazioni che seguono.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Condivisione manuale disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

**Autorizzazione "Visualizza tutti gli utenti"**

Questa autorizzazione si può assegnare agli utenti che devono poter accedere in Lettura a tutti gli utenti, indipendentemente dalle impostazioni di condivisione. A chi dispone già dell'autorizzazione "Gestisci utenti" viene assegnata automaticamente l'autorizzazione "Visualizza tutti gli utenti".

**Impostazioni predefinite a livello di organizzazione per i record utente**

Per impostazione predefinita, questo valore è Privato per gli utenti esterni e Sola lettura pubblica per gli utenti interni. Quando l'accesso predefinito è impostato su Privato, gli utenti possono visualizzare e modificare solo il loro record utente. Gli utenti con subordinati nella gerarchia dei ruoli conservano l'accesso in lettura ai record utente dei subordinati.

**Regole di condivisione utente**

Per le regole di condivisione utente valgono le considerazioni generali sulle regole di condivisione. Le regole di condivisione utente si basano sull'appartenenza a un gruppo pubblico, a un ruolo o a un territorio. Ogni regola di condivisione condivide i membri di un gruppo di origine con quelli del gruppo di destinazione. Prima di creare le regole di condivisione è necessario creare i gruppi pubblici, i ruoli o i territori appropriati. Gli utenti ereditano il medesimo accesso degli utenti che si trovano ai livelli inferiori nella gerarchia dei ruoli.

**Condivisione manuale per i record utente**

La condivisione manuale può concedere l'accesso in lettura o in modifica a un singolo utente, ma solo se l'accesso è più ampio di quello predefinito per l'utente di destinazione. Gli utenti ereditano il medesimo accesso degli utenti che si trovano ai livelli inferiori nella gerarchia dei ruoli. La condivisione gestita Apex non è supportata.

**Condivisioni utente per gli utenti esterni**

Gli utenti dotati di autorizzazione "Gestisci utenti esterni" possono accedere ai record utente esterni per gli utenti di Partner Relationship Management, dell'assistenza clienti e del portale Self-Service clienti, indipendentemente dalle regole di condivisione o dalle impostazioni predefinite dell'organizzazione per i record utente. L'autorizzazione "Gestisci utenti esterni" non consente di accedere agli utenti guest o agli utenti esterni Chatter.

**Compatibilità delle Condivisioni utente**

Quando l'impostazione predefinita dell'organizzazione per l'oggetto utente è Privato, le funzioni seguenti non sono supportate integralmente dalle Condivisioni utente.

- Chatter Messenger non può essere utilizzato dagli utenti esterni. È disponibile per gli utenti interni solo quando l'impostazione predefinita dell'organizzazione per l'oggetto Utente è Sola lettura pubblica.
- Previsioni personalizzabili — Gli utenti con l'autorizzazione "Visualizza tutte le previsioni" possono vedere utenti a cui non sono autorizzati ad accedere.
- Salesforce CRM Content — Un utente che può creare librerie può vedere gli utenti a cui non è autorizzato ad accedere quando aggiunge dei membri alle librerie.

- Tipi di rapporto standard — Alcuni rapporti basati su tipi di rapporto standard rendono visibili dati a cui un utente può non essere autorizzato ad accedere. Per ulteriori informazioni, vedere Controllo della visibilità dei rapporti standard.

VEDERE ANCHE:

Panoramica sulle condivisioni utente

## Definizione delle impostazioni predefinite di condivisione dell'organizzazione per i record utente

Definire le impostazioni predefinite di condivisione dell'organizzazione per l'oggetto utente prima di concedere l'accesso.

Per i record utente, il valore predefinito di condivisione dell'organizzazione si può impostare su Privato o Sola lettura pubblica. L'impostazione predefinita deve essere Privato se esiste almeno un utente che non deve poter visualizzare un record.

Si immagini che un'organizzazione abbia utenti interni (dipendenti e agenti di vendita) ed esterni (clienti/utenti dei portali) in vari account di agenti di vendita o del portale con i seguenti requisiti:

- I dipendenti possono vedere chiunque.
- Gli agenti di vendita possono vedere solo i dipendenti, gli altri agenti e i record utente dei loro clienti.
- I clienti possono vedere solo gli altri clienti se rientrano nell'account dello stesso agente di vendita o dello stesso portale.

Per soddisfare questi requisiti, impostare l'accesso esterno predefinito su Privato ed estendere l'accesso mediante regole di condivisione, condivisione manuale o autorizzazioni utente.

Quando questa funzione viene attivata per la prima volta, l'impostazione di accesso predefinita per gli utenti esterni è Privato. L'impostazione predefinita per gli utenti interni è Sola lettura pubblica. Per modificare le impostazioni predefinite dell'organizzazione per l'accesso esterno all'oggetto Utente:

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per impostare l'accesso in condivisione predefinito:
- "Gestisci condivisione"

1. Da Imposta, immettere `Impostazioni di condivisione` nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
2. Fare clic su **Modifica** nella sezione Impostazioni predefinite organizzazione.
3. Selezionare l'accesso predefinito interno ed esterno da utilizzare per i record Utente.

   L'accesso predefinito esterno deve essere uguale a quello interno o più restrittivo.
4. Fare clic su **Salva**.

   Gli utenti hanno accesso in Lettura ai ruoli inferiori nella gerarchia e accesso completo sul loro record Utente.

VEDERE ANCHE:

Panoramica sulle impostazioni predefinite esterne dell'organizzazione

Controllo degli utenti che possono essere visualizzati dagli utenti dei portali o delle comunità

Panoramica sulle condivisioni utente

## Creazione di regole di condivisione utente

È possibile condividere i membri di un gruppo con quelli di un altro gruppo, o condividere gli utenti in base a dei criteri.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare le regole di condivisione:

- "Gestisci condivisione"

Le regole di condivisione utente possono basarsi sull'appartenenza a gruppi pubblici, ruoli o territori o su altri criteri, quali Reparto e Qualifica. Per impostazione predefinita, è possibile definire fino a 300 regole di condivisione utente, tra cui fino a 50 regole di condivisione basate su criteri. Per informazioni su come aumentare questi limiti, rivolgersi a Salesforce.

Le regole di condivisione utente basate sull'appartenenza consentono di condividere i record utente di proprietà dei membri di un gruppo con i membri di un altro gruppo. Prima di creare una regola di condivisione utente basata sull'appartenenza, verificare che i relativi gruppi siano stati creati.

Gli utenti ereditano il medesimo accesso degli utenti che si trovano ai livelli inferiori nella gerarchia dei ruoli.

1. Da Imposta, immettere *`Impostazioni di condivisione`* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
2. Nell'elenco correlato Regole di condivisione utente, fare clic su **Nuovo**.
3. Digitare il **Nome etichetta** e fare clic sul campo **Nome regola** per compilarlo automaticamente.
4. Immettere la **Descrizione**. Questo campo descrive la regola di condivisione. È facoltativo e può contenere fino a 1000 caratteri.
5. Selezionare un tipo di regola.
6. A seconda del tipo di regola selezionata, procedere come segue:
   a. `Basato sull'appartenenza gruppo`—Gli utenti che sono membri di un gruppo si possono condividere con i membri di un altro gruppo. Nella riga `Utenti che sono membri di`, selezionare una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa (o dal campo di ricerca, se la propria organizzazione ha più di 200 gruppi, ruoli o territori).
   b. `Basata sui criteri`—Specificare i criteri Campo, Operatore e Valore che i record devono soddisfare per essere inclusi nella regola di condivisione. I campi disponibili dipendono dall'oggetto selezionato e il valore è sempre un numero o una stringa letterale. Fare clic su **Aggiungi logica dei filtri...** per modificare la relazione predefinita AND tra ciascun filtro.
7. Nella riga `Condividi con`, specificare il gruppo che deve poter accedere ai record utente. Selezionare una categoria dal primo elenco a discesa e un insieme di utenti dal secondo elenco a discesa o dal campo di ricerca.
8. Selezionare l'impostazione di accesso in condivisione per gli utenti.

| Impostazione di accesso | Descrizione |
|---|---|
| Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. Possono vedere gli utenti di destinazione nelle visualizzazioni elenco e nelle ricerche e interagire con loro su Chatter. |
| Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |

9. Fare clic su **Salva**.

VEDERE ANCHE:

Modifica delle regole di condivisione utente

Categorie di regole di condivisione

Panoramica sulle condivisioni utente

## Modifica delle regole di condivisione utente

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per modificare le regole di condivisione:

- "Gestisci condivisione"

Per le regole di condivisione utente basate sull'appartenenza a gruppi, ruoli o territori è possibile modificare solo le impostazioni di accesso. Per le regole di condivisione utente basate su altri criteri, è possibile modificare i criteri e le impostazioni di accesso.

1. Da Imposta, immettere *Impostazioni di condivisione* nella casella Ricerca veloce, quindi selezionare **Impostazioni di condivisione**.
2. Nell'elenco correlato Regole di condivisione utente, fare clic su **Modifica** accanto alla regola che si desidera modificare.
3. Modificare l'etichetta e il nome della regola, se necessario.
4. Se è stata selezionata una regola basata sull'appartenenza a un gruppo, passare alla fase successiva. Se è stata selezionata una regola basata sui criteri, specificare i criteri a cui devono corrispondere i record per essere inclusi nella regola di condivisione. I campi disponibili dipendono dall'oggetto selezionato e il valore deve essere un numero o una stringa letterale. Fare clic su **Aggiungi logica dei filtri...** per modificare la relazione predefinita AND tra ciascun filtro.
5. Selezionare l'impostazione di accesso in condivisione per gli utenti. Il livello **Accesso utente** è valido per gli utenti che fanno parte dei gruppi con cui si imposta la condivisione.

| Impostazione di accesso | Descrizione |
|---|---|
| Sola lettura | Gli utenti possono visualizzare i record ma non possono aggiornarli. |
| Lettura/scrittura | Gli utenti possono visualizzare e aggiornare i record. |

6. Fare clic su **Salva**.

VEDERE ANCHE:

Panoramica sulle condivisioni utente

## Condivisione dei record utente

L'amministratore definisce il modello di condivisione dell'organizzazione e i livelli di accesso predefiniti per i record utente. Se l'accesso predefinito valido per tutta l'organizzazione è impostato su Privato o Sola lettura pubblica, è possibile estendere i privilegi di condivisione per il proprio record utente. Non è invece possibile limitare l'accesso al di sotto dei livelli predefiniti della propria organizzazione.

È possibile condividere i record utente esterni come quelli degli utenti esterni delle comunità e dei Portali Clienti o partner. È possibile anche condividere il record di un utente interno con un utente esterno. Per visualizzare e gestire i dettagli della condivisione, fare clic su **Condivisione** nella pagina dei dettagli dell'utente. La pagina Dettagli condivisione elenca gli utenti, i gruppi, i ruoli e i territori che hanno accesso di condivisione al record utente. In questa pagina è possibile eseguire le seguenti operazioni.

- Per visualizzare un elenco di elementi filtrati, selezionare un elenco predeterminato dall'elenco a discesa `Visualizza` o fare clic su **Crea nuova visualizzazione** per definire le proprie visualizzazioni personalizzate. Per modificare o eliminare le visualizzazioni create, selezionarle dall'elenco a discesa `Visualizza` e fare clic su **Modifica**.
- Concedere l'accesso al record ad altri utenti, gruppi, ruoli o territori facendo clic su **Aggiungi**. Questo metodo di concessione dell'accesso è noto anche come *condivisione manuale* dei record utente.
- Modificare o eliminare la condivisione manuale facendo clic su **Modifica** o **Canc** accanto alla regola.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare i record utente:
- "Lettura" per i record utente

L'amministratore può disabilitare o abilitare la condivisione manuale dei record utente per tutti gli utenti.

VEDERE ANCHE:

Panoramica sulle condivisioni utente

Differenze tra condivisioni utente con condivisione manuale e insiemi di condivisione

## Concessione dell'accesso ai record utente

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per concedere l'accesso al proprio record utente:

- "Lettura" per l'utente con cui si condivide il record

È possibile concedere manualmente l'accesso ai record utente in modo tale che altre persone possano accedervi. Gli utenti ereditano le stesse autorizzazioni degli utenti che si trovano ai livelli inferiori nella gerarchia dei ruoli. La concessione dell'accesso a un record utente rende la pagina dei dettagli dell'utente visibile agli altri. Rende inoltre visibile l'utente nelle ricerche, nelle visualizzazioni elenco e così via.

Il record utente si può condividere manualmente se altri non possono accedervi mediante le impostazioni predefinite a livello di organizzazione, le regole di condivisione o la gerarchia dei ruoli. Se l'accesso si ottiene tramite più metodi, viene mantenuto il livello di accesso più alto. Gli utenti del portale a volume elevato possono essere condivisi con altri utenti utilizzando le condivisioni manuali, ma non nelle regole di condivisione.

1. Da Imposta, immettere *Utenti* nella casella `Ricerca veloce`, quindi selezionare **Utenti**. Fare clic sul nome dell'utente che si desidera condividere.
2. Nella pagina dei dettagli dell'utente, fare clic su **Condivisione**.
3. Fare clic su **Aggiungi**.
4. Selezionare dall'elenco a discesa il gruppo, l'utente, il ruolo o il territorio con cui condividere.
5. Scegliere gli utenti che avranno diritto all'accesso aggiungendoli all'elenco Condividi con.
6. Scegliere il livello di accesso per il record che si sta condividendo.

   I valori possibili sono Lettura/Scrittura o Sola lettura, a seconda delle impostazioni predefinite a livello di organizzazione per gli utenti. È possibile concedere solo un livello di accesso superiore a quello dell'impostazione predefinita a livello di organizzazione.

7. Fare clic su **Salva**.
8. Per modificare l'accesso al record, fare clic su **Modifica** o **Canc** nella pagina Dettagli condivisione dell'utente.

## Controllo degli utenti che possono essere visualizzati dagli utenti dei portali o delle comunità

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per impostare la visibilità agli utenti del portale e della comunità:

- "Gestisci condivisione"

Se l'organizzazione ha abilitato una comunità per cui sono state fornite licenze del portale, le Condivisioni utente sono abilitate automaticamente. Quando le Condivisioni utente sono attive è possibile decidere gli utenti che possono essere visualizzati per impostazione predefinita dagli utenti della comunità. È possibile scegliere un valore predefinito anche per gli eventuali Portali Clienti o Portali partner dell'organizzazione. Gli utenti che si possono vedere a vicenda possono interagire in tutte le comunità o i portali dell'organizzazione. Ad esempio, se si desidera una comunità più privata si può deselezionare la casella di controllo**Visibilità utente della comunità** e utilizzare altre funzioni di condivisione come le regole di condivisione, le condivisioni manuali o l'accesso ai portali.

Si possono scegliere impostazioni predefinite diverse per comunità e portali.

**Comunità**

L'impostazione predefinita iniziale consente agli utenti della comunità di essere visti da tutti gli altri utenti interni ed esterni nelle comunità di cui fanno parte. L'impostazione predefinita si può modificare per permettere agli utenti esterni delle comunità di essere visibili solo a se stessi e ai loro superiori nella gerarchia dei ruoli. Questa impostazione concede l'accesso in sola lettura ed è valida per tutte le comunità dell'organizzazione.

La visibilità agli utenti derivante dalla preferenza **Visibilità utente della comunità** non si eredita tramite la gerarchia dei ruoli. Se un responsabile nella gerarchia dei ruoli non fa parte di una comunità ma il suo subordinato sì, il responsabile non ottiene l'accesso agli altri membri della comunità.

**Portali**

L'impostazione predefinita iniziale consente agli utenti del portale di essere visti dagli altri utenti del portale nello stesso account. L'impostazione si può modificare per permettere agli utenti esterni dei portali di essere visibili solo da se stessi e dai loro superiori nella gerarchia dei ruoli. Questa impostazione concede l'accesso in sola lettura ed è valida per tutti i portali dell'organizzazione.

Nota: Gli utenti dei Portali partner possono accedere anche ai rispettivi channel manager.

1. Da Imposta, immettere `Impostazioni di condivisione` nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
2. Fare clic su **Modifica** nella sezione Impostazioni predefinite organizzazione.
3. Deselezionare la casella di controllo **Visibilità utente del portale** per permettere agli utenti di essere visibili solo da se stessi e dai loro superiori, oppure selezionare la casella per far sì che gli utenti del portale siano visibili a tutti gli altri utenti del portale nello stesso account.
4. Per **Visibilità utente della comunità**, deselezionare la casella di controllo per permettere agli utenti di essere visibili solo a se stessi e ai loro superiori. Selezionare la casella di controllo per far sì che gli utenti della comunità siano visibili a tutti gli altri utenti nelle rispettive comunità.

   Nota: questa opzione compare solo se sono abilitate le Comunità Salesforce.

5. Fare clic su **Salva**.

La selezione di una di queste opzioni è un metodo rapido per ignorare l'impostazione predefinita dell'organizzazione (Privato) per l'accesso esterno all'oggetto Utente da parte degli utenti delle comunità o dei portali.

Dopo avere definito queste impostazioni predefinite, è possibile ampliare l'accesso ad altri utenti in modo selettivo.

VEDERE ANCHE:

Definizione delle impostazioni predefinite di condivisione dell'organizzazione per i record utente
Creazione di regole di condivisione utente
Controllo della visibilità dei rapporti standard
Panoramica sulle condivisioni utente

## Controllo della visibilità dei rapporti standard

È possibile decidere di mostrare o nascondere i rapporti standard che potrebbero rendere visibili dati a cui un utente non è autorizzato ad accedere.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per impostare la visibilità dei rapporti standard:

- "Gestisci condivisione"

È possibile controllare la visibilità dei rapporti basati su tipi di rapporto standard che potrebbero rendere visibili dati di utenti a cui altri utenti non sono autorizzati ad accedere. Quando si abilitano per la prima volta le Condivisioni utente, tutti i rapporti che contengono dati a cui un utente visualizzatore non è autorizzato ad accedere sono nascosti.

1. Da Imposta, immettere `Impostazioni di condivisione` nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
2. Fare clic su **Modifica** nella sezione Impostazioni predefinite organizzazione.
3. Per consentire agli utenti di visualizzare i rapporti basati su tipi di rapporto standard che possono contenere dati a cui non sono autorizzati ad accedere, selezionare la casella di controllo **Visibilità rapporto standard**, o deselezionarla per nascondere questi rapporti.
4. Fare clic su **Salva**.

Se l'impostazione predefinita dell'organizzazione per l'oggetto utente è Privato e la casella di controllo Visibilità rapporto standard è selezionata, chi visualizza il rapporto vede solo i nomi degli utenti a cui non è autorizzato ad accedere. Dettagli quali il nome utente e l'indirizzo email sono nascosti. Quando si deseleziona la casella di controllo **Visibilità rapporto standard**, gli utenti con autorizzazione "Visualizza tutti gli utenti" potranno comunque vedere tutti i rapporti basati su tipi di rapporto standard. Se l'impostazione predefinita dell'organizzazione per l'oggetto utente è Sola lettura pubblica, questi rapporti saranno visibili anche a tutti gli altri utenti.

Importante: quando è in vigore la condivisione delle analitiche, tutti gli utenti all'interno dell'organizzazione dispongono dell'accesso come Visualizzatori alle cartelle dei rapporti e dei cruscotti digitali che vengono condivisi con loro. Gli utenti con qualifica di Responsabile o di Editor per una cartella e quelli con autorizzazioni amministrative aggiuntive possono godere di un accesso più ampio. L'accesso alle cartelle dei singoli utenti dipende dalla combinazione fra accesso alle cartelle e autorizzazioni utente. Per garantire che le cartelle dei rapporti standard siano opportunamente nascoste, eliminare la condivisione di quelle cartelle per tutti gli utenti, quindi deselezionare le caselle di controllo **Visualizza cruscotti digitali nelle cartelle pubbliche** e **Visualizza rapporti nelle cartelle pubbliche** nei profili degli utenti.

VEDERE ANCHE:

Panoramica sulle condivisioni utente

Tipi di rapporto supportati per le Condivisioni utente

## Controllo della condivisione manuale per i record utente

Per consentire o impedire agli utenti di condividere i propri record con altri utenti dell'organizzazione.

È possibile controllare se il pulsante **Condivisione** è visualizzato nelle pagine dei dettagli degli utenti. Questo pulsante consente di concedere l'accesso ai propri record utente. Per nasconderlo o visualizzarlo a tutti gli utenti, procedere come descritto di seguito.

1. Da Imposta, immettere `Impostazioni di condivisione` nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
2. Fare clic su **Modifica** nella sezione Impostazioni predefinite organizzazione.
3. Selezionare la casella di controllo **Condivisione manuale dei record utente** per visualizzare nelle pagine dei dettagli degli utenti il pulsante **Condivisione**, che consente la condivisione dei record utente. Deselezionare la casella di controllo per nascondere il pulsante, impedendo agli utenti di condividere i loro record con altri.
4. Fare clic su **Salva**.

Quando l'impostazione predefinita per gli utenti di tutta l'organizzazione è Solo lettura pubblica, gli utenti hanno accesso in lettura ai record di tutti gli altri utenti, possono vedere gli altri utenti nelle ricerche e nelle visualizzazioni elenco e possono interagire con loro in Chatter e nelle comunità.

Esempio: Ad esempio, si immagini che un utente partner desideri collaborare con l'agente di vendita nelle comunità. Se è stata disabilitata la casella di controllo `Visibilità utente della comunità` nella pagina Impostazioni di condivisione, gli utenti della comunità sono visibili solo a se stessi e ai loro superiori nella gerarchia dei ruoli. Per concedere all'utente partner l'accesso in lettura all'agente di vendita si può utilizzare la condivisione manuale mediante il pulsante **Condivisione**, presente nella pagina dei dettagli utente dell'agente di vendita. Questo accesso consente a entrambi di interagire e di collaborare nelle comunità.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per abilitare o disabilitare la condivisione manuale dei record utente:

- "Gestisci utenti"

VEDERE ANCHE:

Controllo degli utenti che possono essere visualizzati dagli utenti dei portali o delle comunità

## Ripristino delle impostazioni predefinite di visibilità degli utenti

Le Condivisioni utente permettono di controllare quali utenti possono visualizzare gli utenti dell'organizzazione. Le impostazioni predefinite si possono ripristinare se sono già state utilizzate le Condivisioni utente.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Portali e comunità disponibili nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per ripristinare le impostazioni predefinite di visibilità degli utenti:

- "Gestisci condivisione"

Per ripristinare le impostazioni predefinite di visibilità degli utenti:

1. Da Imposta, immettere *`Impostazioni di condivisione`* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
2. Impostare i valori predefiniti a livello di organizzazione su Sola lettura pubblica per l'accesso interno e su Privato per l'accesso esterno.
3. Abilitare l'accesso degli utenti all'account del portale.

   Nella pagina Impostazioni di condivisione, selezionare la casella di controllo **Visibilità utente del portale**. Questa opzione consente agli utenti del Portale Clienti di vedere gli altri utenti dello stesso account del portale. Gli utenti del Portale partner possono inoltre vedere il titolare dell'account del portale.
4. Abilitare l'accesso di rete per i membri.

   Nella pagina Impostazioni di condivisione, selezionare la casella di controllo **Visibilità utente della comunità**. Questa opzione consente ai membri delle comunità di essere visti da tutti gli altri utenti delle loro comunità.
5. Eliminare le regole di condivisione utente.

   Nella pagina Impostazioni di condivisione, fare clic su **Canc** accanto a tutte le regole di condivisione utente disponibili.
6. Eliminare l'accesso HVPU ai record utente.

   Nella pagina Impostazione Portale Clienti, fare clic su **Canc** accanto a tutti gli insiemi di condivisione disponibili per HVPU.

Dopo che sono state ripristinate le impostazioni predefinite di visibilità degli utenti, tutti gli utenti interni possono vedersi tra loro, gli utenti del portale nello stesso account del portale possono vedersi tra loro e i membri di una stessa comunità possono vedersi tra loro.

VEDERE ANCHE:

Controllo degli utenti che possono essere visualizzati dagli utenti dei portali o delle comunità

Panoramica sulle condivisioni utente

## Tipi di rapporto supportati per le Condivisioni utente

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

I rapporti basati su tipi di rapporto standard potrebbero rendere visibili dati a cui un utente non è autorizzato ad accedere.

I seguenti tipi di rapporto potrebbero contenere dati di utenti a cui chi visualizza il rapporto non è autorizzato ad accedere.

- Account
- Titolari account
- Account con asset
- Account con oggetti personalizzati
- Account con partner
- Utilizzo API

- Campagne con opportunità
- Previsioni personalizzabili: Cronologia previsioni
- Previsioni personalizzabili: Previsioni opportunità
- Opportunità oggetto personalizzato con preventivi
- Eventi con invitati
- Opportunità
- Cronologia campi opportunità
- Cronologia opportunità
- Trend opportunità
- Opportunità e connessioni
- Opportunità con concorrenti
- Opportunità con ruoli referenti
- Opportunità con ruoli referenti e prodotti
- Opportunità con oggetti personalizzati
- Opportunità con partner
- Opportunità con prodotti
- Opportunità con prodotti e pianificazioni
- Opportunità con preventivi e documenti di preventivi
- Opportunità con preventivi e voci preventivo
- Opportunità con team vendite
- Opportunità con team vendite e prodotti
- Opportunità ripartite
- Opportunità ripartite con prodotti
- Opportunità ripartite con prodotti e pianificazioni

Per impostazione predefinita, questi rapporti sono accessibili solo agli utenti dotati del livello di accesso adeguato. È possibile tuttavia modificare questa impostazione per consentire di visualizzare questi rapporti agli utenti sprovvisti di un livello di accesso adeguato agli utenti in questione.

Inoltre, alcuni rapporti possono visualizzare il ruolo di un utente. In questi rapporti, un utente che vede un record ma non è autorizzato ad accedere al suo titolare può vedere il ruolo del titolare.

VEDERE ANCHE:

Controllo della visibilità dei rapporti standard

Panoramica sulle condivisioni utente

## Differenze tra condivisioni utente con condivisione manuale e insiemi di condivisione

La condivisione manuale e gli insiemi di condivisione consentono l'accesso a gruppi di utenti diversi.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Se l'organizzazione ha abilitato le condivisioni utente, è possibile controllare quali utenti vede ciascun utente dell'organizzazione, compresi gli utenti interni ed esterni. La condivisione manuale e gli insiemi di condivisione garantiscono un livello di accesso aggiuntivo rispetto alle impostazioni predefinite e alle regole di condivisione valide per tutta l'organizzazione. Gli utenti esterni come gli utenti del portale a volume elevato (HVPU) e gli utenti delle comunità non hanno ruoli e non si possono utilizzare nelle regole di condivisione.

Esempio: Per concedere agli utenti interni e non HVPU l'accesso a un utente, creare una condivisione manuale con il pulsante Condivisione nella pagina dei dettagli di quell'utente. Concedere agli HVPU l'accesso agli altri utenti creando un insieme di condivisione per i propri portali o comunità.

La tabella riportata sotto mostra quando utilizzare la condivisione manuale e quando gli insiemi di condivisione.

| | Utenti a cui si concede l'accesso | | |
|---|---|---|---|
| | **Interni** | **Non HVPU**[1] | **HVPU**[2] |
| **Interni** | Condivisione manuale | Condivisione manuale | Insieme di condivisione |
| **Non HVPU** | Condivisione manuale | Condivisione manuale | Insieme di condivisione |
| **HVPU** | Condivisione manuale | Condivisione manuale | Insieme di condivisione |

[1] Non HVPU indica un utente esterno che non utilizza un profilo HVPU.

[2] HVPU indica un utente esterno con uno dei seguenti profili:

- Sito Web autenticato
- Utente Comunità Clienti
- Utente di accesso Comunità Clienti
- Portale clienti a volume elevato
- Portale a volume elevato
- Utente Overage Authenticated Website
- Utente Overage High Volume Customer Portal

VEDERE ANCHE:

Panoramica sulle condivisioni utente

Condivisione dei record utente

## Considerazioni sulla condivisione

Informazioni sulle modalità con cui i modelli di condivisione consentono l'accesso ai record agli utenti che non ne sono titolari.

Il modello di condivisione è una complessa relazione tra gerarchie dei ruoli, autorizzazioni utente, regole di condivisione ed eccezioni per alcune situazioni. Prima di impostare il modello di condivisione, rivedere i punti seguenti:

## Eccezioni alla condivisione basata sulla gerarchia dei ruoli

Gli utenti possono visualizzare e modificare sempre tutti i dati di cui sono titolari o che condividono con utenti che occupano una posizione subordinata nella gerarchia dei ruoli. Le eccezioni includono:

- Un'opzione delle impostazioni predefinite dell'organizzazione consente di ignorare le gerarchie quando si determina l'accesso ai dati.
- I referenti non collegati a un account sono sempre riservati. Solo gli amministratori e il titolare del referente possono visualizzarlo. Le regole di condivisione dei referenti non sono valide per i referenti privati.
- Note e allegati contrassegnati come privati tramite la casella di controllo `Privato` sono accessibili solo alla persona che li ha allegati e agli amministratori.
- Gli eventi contrassegnati come privati tramite la casella di controllo `Privato` sono accessibili solo al titolare dell'evento. Quando visualizzano il calendario del titolare dell'evento, gli altri utenti non possono vedere i dettagli degli eventi. Gli utenti che dispongono dell'autorizzazione "Visualizza tutti i dati" oppure "Modifica tutti i dati" possono tuttavia vedere i dettagli degli eventi privati nei rapporti e nelle ricerche oppure quando visualizzano i calendari di altri utenti.
- Gli utenti che nella gerarchia dei ruoli sono a un livello superiore rispetto a un titolare di record possono visualizzare o modificare i record di quel titolare solo se dispongono di autorizzazioni oggetto di "Lettura" o "Modifica" per il tipo di record.
- La visibilità agli utenti derivante dalla preferenza **Visibilità utente della comunità** non si eredita tramite la gerarchia dei ruoli. Se un responsabile nella gerarchia dei ruoli non fa parte di una comunità ma il suo subordinato sì, il responsabile non ottiene l'accesso agli altri membri della comunità. Questo vale solo se nell'organizzazione è abilitato Comunità Salesforce.

## Eliminazione di record

- La facoltà di eliminare singoli record è controllata dagli amministratori, dal titolare del record, dagli utenti che nella gerarchia dei ruoli si trovano in una posizione superiore rispetto al titolare del record, e da qualsiasi utente cui sia stato concesso l'"Accesso completo".
- Se il modello di condivisione è impostato su Lettura/Scrittura/Trasferimento pubblico per i casi o i lead oppure Accesso pubblico completo per le campagne, qualsiasi utente potrà eliminare tali tipi di record.

## Aggiunta di elementi correlati a un record

- Per aggiungere note o allegati a un record, è necessario disporre almeno di accesso in "Lettura/Scrittura" al record.
- Per aggiungere attività o altri record associati a un record, è necessario disporre almeno di accesso in "Lettura" al record.

## Aggiunta o eliminazione manuale dell'accesso in condivisione

- La facoltà di estendere manualmente l'accesso a singoli record è controllata dagli amministratori, dal titolare del record, dagli utenti che nella gerarchia dei ruoli si trovano in una posizione superiore rispetto al titolare del record e da qualsiasi utente cui sia stato concesso l'"Accesso completo".
- La modifica del modello di condivisione comporta l'eliminazione di tutte le condivisioni manuali eventualmente create dagli utenti.

## Autorizzazioni utente e a livello di oggetto

Mentre il modello di condivisione dell'utente controlla la possibilità di visualizzare i record, le autorizzazioni utente e le autorizzazioni a livello di oggetto controllano le azioni che gli utenti possono eseguire su quei record.

- Indipendentemente dalle impostazioni di condivisione, gli utenti devono disporre delle autorizzazioni appropriate a livello di oggetto. Ad esempio, se si condivide un account con altri utenti, tali utenti possono vedere l'account solo se dispongono dell'autorizzazione "Lettura" per gli account. Analogamente, utenti che dispongono dell'autorizzazione "Modifica" per i referenti potrebbero non essere in grado di modificare referenti di cui non sono titolari se lavorano in un modello di condivisione Privato.
- Gli amministratori e gli utenti che dispongono dell'autorizzazione "Visualizza tutti i dati" o "Modifica tutti i dati" hanno accesso alla visualizzazione o modifica di tutti i dati.

## Condivisione di account

- Per limitare l'accesso degli utenti ai record di cui non sono titolari ma che sono associati ad account di cui sono titolari, impostare il livello di accesso appropriato nel ruolo. Ad esempio, è possibile limitare l'accesso degli utenti alle opportunità di cui non sono titolari ma che sono associate ad account di cui sono titolari mediante l'opzione `Accesso opportunità`.
- Indipendentemente dalle impostazioni predefinite valide per tutta l'organizzazione, gli utenti possono, come minimo, visualizzare gli account nei propri territori. Inoltre, è possibile concedere agli utenti l'accesso per visualizzare e modificare i referenti, le opportunità e i casi associati agli account dei loro territori.

## Condivisione di Apex

Non è possibile trasformare da private a pubbliche le impostazioni predefinite a livello di organizzazione di un oggetto personalizzato se Apex code utilizza le voci di condivisione associate a tale oggetto. Ad esempio, se Apex code recupera gli utenti e i gruppi che accedono in condivisione a un oggetto personalizzato Invoice__c (rappresentato come `Invoice__share` nel codice), non è possibile trasformare da privata a pubblica l'impostazione di condivisione dell'oggetto valida per tutta l'organizzazione.

## Condivisione di campagne

- Nelle versioni Enterprise Edition, Unlimited Edition, Performance Edition e Developer Edition, designare tutti gli utenti come Utenti Marketing quando si abilita la condivisione delle campagne. In questo modo si semplificano i processi di amministrazione e risoluzione degli errori, poiché è possibile controllare l'accesso utilizzando condivisione e profili.

  **Nota:** i clienti della versione Professional Edition non possono gestire gli utenti in modo analogo, perché nelle organizzazioni Professional Edition non sono abilitati i profili personalizzati.

- Per segmentare la visibilità tra unità aziendali mantenendo inalterato il comportamento esistente all'interno di un'unità aziendale:
  1. Impostare il valore predefinito per le campagne per tutta l'organizzazione su Privato.
  2. Creare una regola di condivisione per concedere agli utenti marketing l'Accesso completo pubblico a tutte le campagne di proprietà di utenti all'interno della rispettiva unità aziendale.
  3. Creare una regola di condivisione per concedere a tutti gli utenti non marketing di un'unità aziendale l'accesso in sola lettura a tutte le campagne di cui sono titolari utenti all'interno della rispettiva unità aziendale.
- Quando un utente, ad esempio un responsabile marketing regionale, è titolare di più campagne e ha bisogno di segmentarne la visibilità tra più unità aziendali, è necessario condividere le campagne singolarmente anziché utilizzare le regole di condivisione. Le regole di condivisione si applicano a tutte le campagne di cui è titolare un utente e non consentono di segmentarne la visibilità.
- Creare tutte le regole di condivisione delle campagne prima di modificare l'impostazione predefinita a livello di organizzazione per ridurre l'effetto della modifica sui propri utenti.
- Per condividere tutte le campagne dell'organizzazione con un gruppo di utenti o un ruolo specifico, creare una regola di condivisione che si applichi alle campagne di cui sono titolari i membri del gruppo pubblico "Intera organizzazione".
- Ridurre al minimo le regole di condivisione che è necessario creare utilizzando l'opzione "Ruoli e subordinati" anziché scegliere uno specifico ruolo.

- Se le statistiche della gerarchia campagne sono aggiunte al layout di pagina, un utente può visualizzare i dati aggregati relativi a una campagna controllante e a tutte le campagne di livello subordinato all'interno della gerarchia, indipendentemente dal fatto che un utente disponga dell'autorizzazione alla condivisione di una determinata campagna all'interno della gerarchia campagne. Pertanto, tenere presenti le impostazioni di condivisione delle campagne dell'organizzazione quando si abilitano le statistiche della gerarchia campagne. Se non si desidera che gli utenti possano visualizzare i dati aggregati della gerarchia, rimuovere parzialmente o totalmente i campi delle statistiche della gerarchia campagne dall'elenco correlato Gerarchia campagne. Tali campi continueranno a essere disponibili ai fini della generazione di rapporti.
- Se il modello di condivisione è impostato su Accesso completo pubblico per le campagne, qualsiasi utente può eliminare quei tipi di record.

## Condivisione dei membri delle campagne

La condivisione dei membri delle campagne è controllata dalle regole di condivisione delle campagne. Gli utenti che possono visualizzare una campagna possono visualizzare anche i membri delle campagne associate.

## Condivisione di referenti

- L'impostazione predefinita di condivisione di tutta l'organizzazione per i referenti non è disponibile per le organizzazioni in cui sono abilitati gli account personali.
- Se l'impostazione predefinita di tutta l'organizzazione per i referenti è Controllata da società controllante, le opzioni `Accesso referente` non sono disponibili quando si condividono record correlati come gli account; l'accesso ai referenti è invece determinato dall'accesso dell'utente all'account del referente.

## Condivisione di listini prezzi

- Le impostazioni di condivisione dei listini determinano se gli utenti possono aggiungere il listino e i relativi prodotti alle opportunità.
- Le autorizzazioni utente determinano se gli utenti possono visualizzare, creare, modificare ed eliminare listini prezzi.

VEDERE ANCHE:

Panoramica sulle impostazioni di condivisione

## Visualizzazione delle precedenze di condivisione

Quando si seleziona un oggetto nella pagina Impostazioni di condivisione, la pagina comprende un elenco correlato Precedenze condivisione che mostra gli eventuali profili che ignorano le impostazioni di condivisione per quell'oggetto.

Per visualizzare l'elenco Precedenze condivisione, da Imposta immettere *Impostazioni di condivisione* nella casella Ricerca veloce, quindi selezionare **Impostazioni di condivisione**. Selezionare poi un oggetto dall'elenco Gestisci impostazioni di condivisione per.

Per ciascun profilo l'elenco specifica le autorizzazioni che gli consentono di ignorare le impostazioni di condivisione. Le autorizzazioni "Visualizza tutti i dati" e "Modifica tutti i dati" consentono di ignorare le impostazioni di condivisione per tutti gli oggetti dell'organizzazione, mentre le autorizzazioni "Visualizza tutto" e "Modifica tutto" consentono di ignorare le impostazioni di condivisione per l'oggetto denominato.

Nota: l'elenco Precedenze condivisione non mostra le autorizzazioni concesse tramite gli insiemi di autorizzazioni, che consentono di ignorare anche le impostazioni di condivisione per un oggetto.

Per ignorare le impostazioni di condivisione per oggetti specifici, è possibile creare o modificare insiemi di autorizzazioni o profili e abilitare le autorizzazioni relative agli oggetti "Visualizza tutto" e "Modifica tutto". Queste autorizzazioni forniscono accesso a tutti i record associati a un oggetto in tutta l'organizzazione, indipendentemente dalle impostazioni di condivisione. Prima di impostare queste autorizzazioni, confrontare le diverse modalità di controllo dell'accesso ai dati.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le precedenze di condivisione:

- "Visualizza impostazione e configurazione"

VEDERE ANCHE:

Profili

# Calcoli delle condivisioni

## Ricalcolo delle regole di condivisione

Quando si apportano modifiche a gruppi, ruoli e territori, le regole di condivisione vengono in genere rivalutate automaticamente per aggiungere o rimuovere l'accesso in funzione delle necessità. Le modifiche possono includere l'aggiunta o la rimozione di singoli utenti da un gruppo, un ruolo o un territorio, la modifica del ruolo a cui fa capo un determinato ruolo, la modifica del territorio a cui è subordinato un determinato territorio o l'aggiunta o la rimozione di un gruppo interno a un altro gruppo.

Nota: non è necessario ricalcolare ogni volta che si modifica o si crea una regola di condivisione. I pulsanti Ricalcola degli elenchi correlati Regole di condivisione devono essere utilizzati solo se gli aggiornamenti delle regole di condivisione non sono riusciti o non funzionano come previsto. L'amministratore riceverà un messaggio di notifica se gli aggiornamenti delle regole di condivisione non sono riusciti.

Per ricalcolare manualmente le regole di condivisione per un oggetto:

1. Da Imposta, immettere *Impostazioni di condivisione* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di condivisione**.
2. Nell'elenco correlato Regole di condivisione dell'oggetto desiderato, fare clic su **Ricalcola**.
3. Per monitorare l'andamento di un ricalcolo, da Imposta immettere *Processi in background* nella casella `Ricerca veloce`, quindi selezionare **Processi in background**.

Nota: il pulsante **Ricalcola** è disabilitato quando vengono rinviati i calcoli dell'appartenenza ai gruppi o delle regole di condivisione. Le regole di condivisione per gli oggetti correlati vengono ricalcolate automaticamente; ad esempio, le regole di condivisione account vengono ricalcolate al ricalcolo delle regole di condivisione opportunità, poiché i record opportunità sono in relazione record principale-record dettaglio sui record account.

Quando viene ricalcolata la condivisione, Salesforce esegue anche tutti i ricalcoli di condivisione Apex. Durante il ricalcolo delle regole di condivisione vengono calcolate anche le regole di condivisione degli oggetti correlati. A ricalcolo concluso si riceverà un'email di notifica. Ad esempio, quando si ricalcola una regola di condivisione per le opportunità vengono ricalcolate anche le regole di condivisione account poiché le opportunità sono il lato dettaglio di un oggetto account.

Il calcolo automatico delle regole di condivisione è abilitato per impostazione predefinita. È possibile rinviare il calcolo delle regole di condivisione sospendendolo e riprendendolo a propria discrezione.

VEDERE ANCHE:

Panoramica sulle regole di condivisione
Panoramica sul rinvio dei calcoli di condivisione
Monitoraggio dei processi in background
Ricalcolo parallelo asincrono delle regole di condivisione

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Le regole di condivisione di account e referenti sono disponibili nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Le regole di condivisione territorio account, caso, lead, opportunità, ordine e oggetto personalizzato sono disponibili nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Le regole di condivisione delle campagne sono disponibili nella versione **Professional Edition** con un supplemento di prezzo, e inoltre nelle versioni **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**.

AUTORIZZAZIONI UTENTE

Per ricalcolare le regole di condivisione:

- "Gestisci condivisione"

## Ricalcolo parallelo asincrono delle regole di condivisione

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Per rendere più rapido il ricalcolo delle regole di condivisione si può eseguirlo in modo asincrono e in parallelo.

Quando si creano, si aggiornano o si eliminano regole di condivisione, il ricalcolo che ne deriva viene ora elaborato in modo asincrono e in parallelo. Il ricalcolo viene eseguito in background in modo parallelo e asincrono, abbreviando il processo e garantendo migliore flessibilità per le operazioni sul sito quali applicazione di patch e riavvii del server. Al termine del ricalcolo viene inviato un messaggio email di notifica. Finché il ricalcolo non è terminato, non è possibile eseguire altre operazioni di condivisione quali la creazione di una regola di condivisione o l'aggiornamento delle impostazioni predefinite dell'organizzazione.

Il ricalcolo in parallelo delle regole di condivisione viene eseguito anche nei seguenti casi.

- Quando si fa clic sul pulsante Ricalcola delle regole di condivisione nella pagina Impostazioni di condivisione
- Quando si ricalcolano le regole di condivisione nella pagina Rinvia calcoli condivisione

È possibile monitorare l'andamento del ricalcolo in parallelo nella pagina Processi in background, oppure visualizzare le operazioni di condivisione più recenti nella pagina Visualizza itinerario di controllo impostazioni.

Il ricalcolo delle regole di condivisione mantiene la condivisione implicita fra account e record secondari. Nella pagina Processi in background, questi processi corrispondono ai seguenti sottotipi di processo: **Account — Rimozione accesso extra controllante** e **Account — Concessione accesso controllante**. Inoltre, l'eliminazione di una regola di condivisione corrisponde al sottotipo di processo **Oggetto — Pulitura accesso**, che indica che le righe di condivisione non rilevanti vengono eliminate.

Nota: per una trattazione approfondita dell'accesso ai record, vedere *Designing Record Access for Enterprise Scale*.

VEDERE ANCHE:

Monitoraggio dei processi in background

Ricalcolo delle regole di condivisione

Comportamento di condivisione incorporato

## Panoramica sul rinvio dei calcoli di condivisione

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Nota: per impostazione predefinita, la funzione di rinvio dei calcoli di condivisione è disabilitata. Per abilitarla nella propria organizzazione, contattare Salesforce.

Se si apportano molte modifiche alla configurazione, la valutazione delle regole di condivisione può diventare estremamente lunga o generare errori di timeout. Per evitare questi inconvenienti, l'amministratore può sospendere questi calcoli e riprenderli durante un periodo di manutenzione dell'organizzazione.

Il rinvio dei calcoli di condivisione è perfetto per i casi in cui si apportano numerose modifiche a ruoli, territori, gruppi, utenti, proprietà degli account portale o gruppi pubblici che partecipano alle regole di condivisione e si desidera sospendere il calcolo di condivisione automatico per riprenderlo in un secondo momento.

Il calcolo di appartenenza ai gruppi e delle regole di condivisione è abilitato per impostazione predefinita.

| Se | È possibile |
| --- | --- |
| Il calcolo di appartenenza ai gruppi e delle regole di condivisione è abilitato | • Sospendere, aggiornare e riprendere il calcolo di appartenenza ai gruppi. In questo modo si sospende il calcolo delle regole di condivisione e si rende necessario un ricalcolo completo delle stesse.<br>• Sospendere, aggiornare e riprendere il calcolo delle regole di condivisione. |
| Il calcolo di appartenenza ai gruppi è abilitato e il calcolo delle regole di condivisione è sospeso | Sospendere, aggiornare e riprendere il calcolo di appartenenza ai gruppi. |
| Il calcolo di appartenenza ai gruppi è sospeso e il calcolo delle regole di condivisione è abilitato | Sospendere, aggiornare, riprendere ed eseguire nuovamente il calcolo delle regole di condivisione. |

Per sospendere o riprendere il calcolo di appartenenza ai gruppi, vedere Gestione dei calcoli di appartenenza ai gruppi.

Per sospendere, riprendere o effettuare nuovamente il calcolo delle regole di condivisione, vedere Rinvio dei calcoli delle regole di condivisione.

VEDERE ANCHE:

Ricalcolo delle regole di condivisione

## Gestione dei calcoli di appartenenza ai gruppi

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per rinviare (sospendere e riprendere) i calcoli di condivisione:

- "Gestisci utenti"

  E

  "Gestisci rinvio dei calcoli di condivisione"

Quando si apportano modifiche a ruoli, territori, gruppi o utenti o si modifica la proprietà degli account portale, l'appartenenza ai gruppi viene ricalcolata automaticamente per eliminare o aggiungere l'accesso in funzione delle esigenze. Le modifiche possono comportare l'aggiunta o la rimozione di un utente da un gruppo o la modifica di un ruolo per consentire l'accesso a gruppi diversi di rapporti.

In caso di modifiche ai gruppi che interessano un numero notevole di record può essere opportuno sospendere il calcolo automatico di appartenenza ai gruppi e riprenderlo in un secondo momento. Tenere presente che, se non si riprende il calcolo, potrebbero verificarsi delle discrepanze nelle condivisioni dei record.

Per sospendere o riprendere i calcoli di appartenenza ai gruppi:

1. Da Imposta, immettere *Rinvia calcoli condivisione* nella casella `Ricerca veloce`, quindi selezionare **Rinvia calcoli condivisione**.
2. Nell'elenco correlato Calcoli di appartenenza gruppo, fare clic su **Sospendi**.

   Nota: la sospensione dei calcoli di appartenenza ai gruppi determina anche la sospensione dei calcoli delle regole di condivisione, se questi sono abilitati. Inoltre, per riprendere i calcoli di appartenenza ai gruppi è necessario il ricalcolo completo delle regole di condivisione.

3. Apportare le modifiche desiderate ai ruoli, ai territori, ai gruppi, agli utenti o alla proprietà degli account portale.

4. Per abilitare il calcolo di appartenenza ai gruppi, fare clic su **Riprendi**.

VEDERE ANCHE:

Panoramica sul rinvio dei calcoli di condivisione

## Rinvio dei calcoli delle regole di condivisione

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Le regole di condivisione di account e referenti sono disponibili nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Le regole di condivisione territorio account, caso, lead e opportunità sono disponibili nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Le regole di condivisione delle campagne sono disponibili nella versione **Professional Edition** con un supplemento di prezzo, e inoltre nelle versioni **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**.

Le regole di condivisione oggetti personalizzati sono disponibili nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**.

Nota: per impostazione predefinita, la funzione di rinvio dei calcoli di condivisione è disabilitata. Per abilitarla nella propria organizzazione, contattare Salesforce.

AUTORIZZAZIONI UTENTE

Per rinviare (sospendere e riprendere) e ricalcolare le regole di condivisione:

- "Gestisci utenti"

  E

  "Gestisci rinvio dei calcoli di condivisione"

Per sospendere, riprendere o effettuare nuovamente il calcolo delle regole di condivisione:

1. Da Imposta, immettere *Rinvia calcoli condivisione* nella casella `Ricerca veloce`, quindi selezionare **Rinvia calcoli condivisione**.
2. Nell'elenco correlato Calcoli regole di condivisione, fare clic su **Sospendi**.
3. Apportare le modifiche alle regole di condivisione, ai ruoli, ai territori o ai gruppi pubblici che partecipano alle regole di condivisione.

   Nota: tutte le modifiche apportate alle regole di condivisione richiedono un ricalcolo completo.

   Per abilitare il calcolo delle regole di condivisione, fare clic su **Riprendi**.
4. Per ricalcolare manualmente le regole di condivisione, fare clic su **Ricalcola**.

Prendere in considerazione il rinvio dei calcoli di condivisione prima di eseguire aggiornamenti di grande entità delle regole di condivisione. Quando viene ricalcolata la condivisione, Salesforce esegue anche tutti i ricalcoli di condivisione Apex.

VEDERE ANCHE:

Gestione dei calcoli di appartenenza ai gruppi

## Blocco delle condivisioni specifico di un oggetto (programma pilota)

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Quando si crea, si modifica o si elimina una regola di condivisione viene eseguito un ricalcolo per aggiornare l'accesso ai record nell'organizzazione. Se gli utenti sono numerosi e i volumi di dati ingenti, questa operazione può richiedere parecchio tempo. La funzione di blocco delle condivisioni specifico di un oggetto consente di modificare una regola di condivisione per altri oggetti senza aspettare la conclusione del ricalcolo per tutti gli oggetti. A seconda dell'oggetto, del tipo di regola di condivisione e del gruppo di utenti di destinazione, le regole di condivisione per un altro oggetto o per lo stesso oggetto si possono modificare tramite l'interfaccia utente o l'API.

Nota: questa funzione viene fornita a clienti selezionati tramite un programma pilota che richiede l'accettazione di condizioni specifiche. Per poter partecipare al programma, rivolgersi a Salesforce. Poiché i programmi pilota sono soggetti a modifiche, non possiamo garantire l'accettazione della richiesta. Questa funzione pilota non è disponibile al pubblico in generale, come riportato in questo documento, in comunicati stampa o dichiarazioni pubbliche. Non possiamo garantire che questa funzione sarà disponibile al pubblico in generale, né che sarà disponibile entro un determinato periodo di tempo. Si consiglia pertanto di basare le decisioni di acquisto solo sulle funzioni disponibili al pubblico in generale.

Senza il blocco delle condivisioni specifico di un oggetto non è possibile inviare modifiche alle condivisioni simultanee fino alla conclusione del ricalcolo per tutti gli oggetti. Se si intende abilitare il blocco delle condivisioni specifico di un oggetto, tenere presenti le seguenti modifiche nell'organizzazione.

**Regole di condivisione basate su criteri e sulla proprietà**

Il ricalcolo avviene se una regola di condivisione è stata modificata o quando si fa clic sul pulsante **Ricalcola** nella pagina Impostazioni di condivisione. Facendo clic sul questo pulsante si bloccano le regole di condivisione per quell'oggetto (1), ma è comunque possibile apportare modifiche alle regole di condivisione di un altro oggetto.

Nota: non è necessario ricalcolare ogni volta che si modifica o si crea una regola di condivisione. I pulsanti Ricalcola degli elenchi correlati Regole di condivisione devono essere utilizzati solo se gli aggiornamenti delle regole di condivisione non

sono riusciti o non funzionano come previsto. L'amministratore riceverà un messaggio di notifica se gli aggiornamenti delle regole di condivisione non sono riusciti.

Sharing Rules

Lead Sharing Rules New Recalculate Lead Sharing Rules Help

A sharing rule recalculation on Leads has been initiated by Diana Widjaja on 8/10/2015 12:44 PM. You can't submit any changes for Leads prior to the completion of the operation. Diana Widjaja will receive an email when the operation finishes.

| Action | Criteria | Shared With | Lead |
|---|---|---|---|
| Edit \| Del | Lead: Company EQUALS AW Computing | All Internal Users | Read/Write |

1

Account Sharing Rules New Recalculate Account Sharing Rules Help

No sharing rules specified.

Opportunity Sharing Rules New Recalculate Opportunity Sharing Rules Help

| Action | Criteria | Shared With | Opportunity |
|---|---|---|---|
| Edit \| Del | Opportunity: Opportunity Name CONTAINS Acme Computing | All Internal Users | Read Only |

Quando è in corso il ricalcolo di una condivisione basata sulla proprietà non è possibile creare, modificare o eliminare le regole di condivisione basate sulla proprietà di un oggetto dirette al gruppo di utenti interessato. Ad esempio, si immagini di creare una regola di condivisione dei lead basata sulla proprietà diretta a tutti gli utenti interni. È possibile creare, aggiornare o eliminare altre regole di condivisione dei lead basate sulla proprietà dirette a tutti gli utenti interni solo al termine del ricalcolo. A ricalcolo concluso si riceverà un'email di notifica. Tuttavia, è comunque possibile creare altre regole di condivisione dei lead basate sulla proprietà dirette a qualsiasi altro gruppo pubblico tranne il gruppo Tutti gli utenti interni mentre è ancora in corso il ricalcolo dovuto alla creazione della prima regola di condivisione.

Quando è in corso un ricalcolo delle condivisioni basate su criteri non è possibile modificare o eliminare la regola in questione (2). È però possibile creare, modificare o eliminare in contemporanea qualsiasi altra regola di condivisione basata sulla proprietà o su criteri.

Sharing Settings

This page displays your organization's sharing settings. These settings specify the level of access your users have to each others' data.

One or more sharing rule operations has been initiated. See below for additional details.

Sharing Rules

Lead Sharing Rules New Recalculate Lead Sharing Rules Help

A sharing rule operation is currently in progress. The initiating user will receive an email when each operation finishes.

| Action | Criteria | Shared With | Lead |
|---|---|---|---|
| Edit \| Del | Lead: Company EQUALS AW Trading | All Internal Users | Read Only |

2

Le impostazioni predefinite a livello di organizzazione non si possono modificare durante un ricalcolo, e viceversa.

Sharing Settings

This page displays your organization's sharing settings. These settings specify the level of access your users have to each others' data.

An organization-wide default update has been initiated by Diana Widjaja on 8/7/2015 10:40 AM. You can't submit any changes prior to the completion of the operation. Diana Widjaja will receive an email when the operation finishes.

**Account, casi, referenti e opportunità**

Le regole di condivisione possono influire sugli account e sugli oggetti controllati associati (casi, referenti e opportunità) e pertanto questi sono bloccati tutti insieme per garantire la corretta esecuzione del ricalcolo. Ad esempio, se si creano e si modificano delle regole di condivisione degli account non è possibile creare o modificare la regola di condivisione di un caso, di un referente o di un'opportunità. Analogamente, se si crea o si modifica la regola di condivisione di un'opportunità non è possibile creare o modificare la regola di condivisione di un caso, di un referente o di un account prima della conclusione del ricalcolo. Tenere presente che i blocchi non vengono condivisi tra gli oggetti, tranne nel caso degli account e degli oggetti controllati associati.

Nota: facendo clic sul pulsante **Ricalcola** per le regole di condivisione di uno di questi quattro oggetti si impedisce a chiunque di modificare qualsiasi regola di condivisione per quegli oggetti fino alla conclusione del ricalcolo.

Nell'esempio che segue, una regola di condivisione degli account basata sulla proprietà è stata eliminata ed è in corso il ricalcolo. Anche se non è possibile creare, modificare o eliminare un'altra regola di condivisione basata sulla proprietà appartenente a uno qualsiasi di questi oggetti, è possibile modificare una regola di condivisione basata sui criteri (3) appartenente a questi oggetti.

Account Sharing Rules New Recalculate Account Sharing Rules Help

A sharing rule operation is in progress. You can't create new owner-based sharing rules for Accounts targeting the following groups. The initiating user will receive an email when each operation finishes.

| Initiated By | Shared With | Initiated On |
| --- | --- | --- |
| Diana Widjaja | All Internal Users | 8/7/2015 10:14 AM |

No sharing rules specified.

Opportunity Sharing Rules New Recalculate Opportunity Sharing Rules Help

A sharing rule operation is in progress. You can't create new owner-based sharing rules for Opportunities targeting the following groups. The initiating user will receive an email when each operation finishes.

| Initiated By | Shared With | Initiated On |
| --- | --- | --- |
| Diana Widjaja | All Internal Users | 8/7/2015 10:14 AM |

| Action | Criteria | Shared With | Opportunity |
| --- | --- | --- | --- |
| Edit \| Del | Opportunity: Opportunity Name CONTAINS Acme Computing | All Internal Users | Read Only |

3

Case Sharing Rules New Recalculate Case Sharing Rules Help

A sharing rule operation is in progress. You can't create new owner-based sharing rules for Cases targeting the following groups. The initiating user will receive an email when each operation finishes.

| Initiated By | Shared With | Initiated On |
| --- | --- | --- |
| Diana Widjaja | All Internal Users | 8/7/2015 10:14 AM |

No sharing rules specified.

VEDERE ANCHE:

Panoramica sulle regole di condivisione

Ricalcolo delle regole di condivisione

Panoramica sul rinvio dei calcoli di condivisione

## Comportamento di condivisione incorporato

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

La condivisione di account e referenti è disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

La condivisione per casi e opportunità è disponibile nelle versioni **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Salesforce è predisposto per la condivisione implicita tra gli account e i record controllati (opportunità, casi e referenti) e per vari gruppi di utenti del portale.

**Condivisione tra account e record controllati**

- **Accesso a un account controllante**: se si è autorizzati ad accedere a un record controllato di un account, si dispone di accesso implicito in Sola lettura a tale account.
- **Accesso ai record controllati**: se si è autorizzati ad accedere a un account controllante, è possibile accedere ai record controllati associati. Il ruolo del titolare dell'account determina il livello di accesso ai record controllati.

**Comportamento di condivisione per gli utenti dei portali**

- **Accesso ad account e casi**: l'utente del portale di un account dispone di accesso in Sola lettura all'account controllante e a tutti i referenti di tale account.
- **Accesso per la gestione dei dati di proprietà degli utenti del portale Service Cloud**: poiché gli utenti del portale Service Cloud non hanno ruoli, i titolari degli account portale non possono accedere ai loro dati tramite la gerarchia dei ruoli. Per concedere a tali utenti l'accesso ai dati è possibile aggiungere titolari di account al gruppo di condivisione del portale in cui gli utenti del portale Service Cloud stanno lavorando. Questa operazione consente di accedere a tutti i dati di cui gli utenti del portale Service Cloud sono titolari in quel portale.
- **Accesso ai casi**: se un utente del portale è referente per un caso, potrà accedere al caso in modalità Sola lettura.

**Operazioni relative all'appartenenza ai gruppi e ricalcolo condivisione**

Operazioni semplici quali la modifica del ruolo di un utente, lo spostamento di un ruolo in un altro ramo della gerarchia o la modifica del titolare di un account di un portale possono innescare un ricalcolo delle regole di condivisione. Salesforce deve verificare l'accesso ai dati utente per le persone di livello gerarchico superiore al nuovo o al vecchio ruolo dell'utente e aggiungere o eliminare le condivisioni agli eventuali record interessati.

VEDERE ANCHE:

Protezione dell'accesso ai dati

# Risoluzione degli errori di privilegi insufficienti

La maggior parte degli errori di privilegi insufficienti sono causati da un'autorizzazione mancante o da impostazioni di condivisione che impediscono l'accesso a un record o l'esecuzione di un'operazione, ad esempio l'esecuzione di un rapporto.

Un utente potrebbe non disporre dei diritti di accesso appropriati per diversi livelli, ad esempio oggetto, record o processo. Ad esempio, il profilo di un utente potrebbe impedirgli di accedere all'oggetto account, oppure il ruolo di un utente potrebbe impedirgli di accedere a un record caso. È possibile che questo errore venga visualizzato anche quando si fa clic su un link a un record o sulla scheda di una pagina Visualforce a cui non si ha accesso.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte le versioni**

La maggior parte dei casi possono essere risolti utilizzando il pulsante Condivisione sulla pagina dei dettagli del record, che consente di condividere il record con un altro utente, se necessario. Gli amministratori possono anche risolvere il problema utilizzando l'API, ad esempio eseguendo una query sull'oggetto UserRecordAccess per verificare l'accesso di un utente a un insieme di record. Per ulteriori informazioni, vedere *SOAP API Developer's Guide*.

Se questi strumenti non aiutano a risolvere il problema, un amministratore può tentare di procedere alla diagnosi con questo diagramma per la risoluzione dei problemi.

- Risoluzione degli errori di accesso a livello di oggetto tramite la revisione di profili utenti e insiemi di autorizzazioni.
- Risoluzione degli errori di accesso a livello di record tramite la revisione delle impostazioni di condivisione, ad esempio le impostazioni predefinite a livello dell'organizzazione e le regole di condivisione.
- Risoluzione degli errori a livello di processo tramite la revisione delle regole di convalida e dei trigger Apex.

È consigliabile che un amministratore effettui l'accesso all'applicazione utilizzando i dati di accesso dell'utente per aiutarlo a risolvere il problema. È possibile concedere agli amministratori l'accesso per un periodo determinato.

## Risoluzione degli errori di accesso a livello di autorizzazione e di oggetto

Gli errori di privilegi insufficienti possono essere causati dalla mancanza di autorizzazioni a livello di oggetto e di utente. È possibile risolvere questo tipo di errori tramite un profilo utente e un insieme di autorizzazioni.

In generale, il metodo migliore per indagare su problemi di accesso a livello di oggetto e di autorizzazioni è tramite l'API. Tuttavia, è possibile utilizzare la seguente procedura per indagare tramite strumenti "point-and-click".

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte le versioni**

AUTORIZZAZIONI UTENTE

Per visualizzare i profili e gli insiemi di autorizzazioni:
- "Visualizza impostazione e configurazione"

Per modificare le autorizzazioni oggetto:
- "Gestisci profili e insiemi di autorizzazioni"

  E

  "Personalizza applicazione"

1. Verificare le autorizzazioni a livello di oggetto nel profilo dell'utente.

   Le autorizzazioni oggetto, configurate sui profili e gli insiemi di autorizzazioni, determinano quali oggetti un utente può leggere, creare, modificare o eliminare.

   a. Nella pagina dei dettagli dell'utente, fare clic sul profilo utente.

   b. Nella pagina con la panoramica dei profili, accedere a **Impostazioni oggetti** o **Autorizzazioni oggetti**.

      Prendere nota delle autorizzazioni per l'oggetto. Ad esempio, se l'utente sta tentando di visualizzare un account, verificare che sia abilitata l'autorizzazione "Lettura" per gli oggetti account e referente sul profilo utente.

      Oppure, se l'utente sta tentando di eseguire un rapporto, potrebbe non essere in possesso dell'autorizzazione "Lettura" su un oggetto al quale fa riferimento il rapporto.

2. Verificare le autorizzazioni utente in uno dei modi seguenti, a seconda dell'interfaccia utente del proprio profilo.

- Nell'interfaccia utente profilo ottimizzata, rivedere le autorizzazioni nelle sezioni Autorizzazioni applicazione e Autorizzazioni di sistema.
- Nell'interfaccia utente profilo originale, rivedere le autorizzazioni in Autorizzazioni amministrative e Autorizzazioni utente generali.

Prendere nota delle autorizzazioni utente pertinenti. Ad esempio, se l'utente sta tentando di inviare un'email a un lead, verificare che sia abilitata l'autorizzazione "Invia email".

3. Verificare le autorizzazioni negli insiemi di autorizzazioni dell'utente.
   a. Nella pagina dei dettagli dell'utente, scorrere fino all'elenco correlato Assegnazioni insieme di autorizzazioni e fare clic su ciascun insieme di autorizzazioni.
   b. Nella pagina della panoramica dell'insieme di autorizzazioni, fare clic su Impostazioni oggetti e rivedere le autorizzazioni oggetto assegnate.
   c. Rivedere le autorizzazioni utente nelle sezioni Autorizzazioni applicazione e Autorizzazioni di sistema.
   d. Ripetere questa procedura per ogni insieme di autorizzazioni assegnato all'utente.
4. Se necessario, assegnare l'autorizzazione richiesta utilizzando un insieme di autorizzazioni o aggiornando il profilo. Gli insiemi di autorizzazioni consentono l'accesso su base individuale. Assegnare autorizzazioni sul profilo utente *solo* se tutti gli utenti di questo profilo necessitano dell'accesso. Assicurarsi di osservare i criteri di protezione dell'organizzazione e intraprendere le azioni di conseguenza.

VEDERE ANCHE:

Risoluzione degli errori di privilegi insufficienti

Insiemi di autorizzazioni

Autorizzazioni e accesso degli utenti

Profili

## Risoluzione degli errori di accesso a livello di record

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte le versioni**

AUTORIZZAZIONI UTENTE

Per creare o modificare le regole di condivisione:
- "Gestisci condivisione"

Per impostare i team:
- “Personalizza applicazione”

Per gestire territori:
- "Gestisci territori"

Gli errori di privilegi insufficienti possono essere causati dalle impostazioni di condivisione, ad esempio dai ruoli o dalle regole di condivisione.

Per verificare se l'errore è a livello di record, attenersi alla seguente procedura. In alternativa, è possibile anche utilizzare l'API per eseguire una query sull'accesso dell'utente a un insieme di record, oppure utilizzare il pulsante Condivisione sulla pagina dei dettagli del record.

1. Se la propria organizzazione utilizza i ruoli, verificare il ruolo dell'utente rispetto al titolare del record.

   Ad esempio, gli utenti possono eliminare i record solo se sono titolari del record, se occupano una posizione superiore nella gerarchia dei ruoli rispetto al titolare del record oppure se ne sono l'amministratore. Analogamente, gli utenti hanno sempre l'accesso in lettura ai record i cui titolari occupano una posizione inferiore nella gerarchia dei ruoli, a meno che non sia deselezionato **Concedi accesso tramite le gerarchie** (solo oggetti personalizzati).

   a. Da Imposta, immettere *Utenti* nella casella `Ricerca veloce`, quindi selezionare **Utenti**.

      Verificare il ruolo dell'utente e quello dell'utente del quale si sta accedendo al record.

      Ad esempio, un utente non può eliminare o unire gli account di proprietà di un utente che si trova in una gerarchia dei ruoli non correlata, anche se dispone delle autorizzazioni appropriate sugli oggetti.

2. Se l'utente dovrebbe aver ottenuto l'accesso tramite una regola di condivisione, rivedere le proprie regole di condivisione.

   È possibile che l'utente sia stato escluso involontariamente da una regola di condivisione.

   a. Da Imposta, immettere *Impostazioni di condivisione* nella casella Ricerca veloce, quindi selezionare **Impostazioni di condivisione**.
   b. Verificare il gruppo pubblico (o altre categorie come ruoli o aree di attesa) al quale l'utente dovrebbe appartenere per quella specifica regola di condivisione.

3. Verificare i propri team di vendita.

   Se la propria organizzazione utilizza i team per account, opportunità o casi, è possibile che l'utente non sia stato considerato durante l'impostazione dei team. Controllare i team per determinare se l'utente avrebbe dovuto ottenere l'accesso tramite un team.

   a. Da imposta, immettere il team che si desidera verificare, ad esempio *Team account*, nella casella Ricerca veloce, quindi selezionare il team.

      Aggiungere l'utente al team, se appropriato.

4. Controllare le condivisioni manuali.

   L'utente potrebbe aver ottenuto l'accesso tramite una condivisione manuale, ma aver perso tale accesso in seguito al cambiamento del titolare del record, determinando così l'eliminazione automatica della condivisione manuale. È anche possibile che la condivisione manuale sia stata eliminata con il pulsante **Condivisione** nella pagina dei dettagli del record. Le condivisioni manuali in un record possono essere create o rimosse solo dal titolare del record, da un amministratore o da un utente di grado superiore al titolare nella gerarchia dei ruoli.

   a. Nella pagina dei dettagli del record, fare clic su **Condivisione**.

      La pagina Dettagli condivisione mostra gli utenti, i gruppi, i ruoli e i territori che hanno accesso al record.

   b. Se l'utente deve ottenere l'accesso tramite una condivisione manuale, creare una condivisione manuale facendo clic su **Aggiungi**.

5. Riesaminare i territori.

   Se l'organizzazione utilizza i territori, è possibile che l'utente non sia presente nei territori o che il record non si trovi nel territorio corretto in cui l'utente è un membro. In caso contrario, si deve essere un responsabile previsione, è stata selezionata l'opzione Responsabili previsione possono gestire territori e si sta lavorando in una posizione inferiore alla propria nella gerarchia dei territori.

VEDERE ANCHE:

Risoluzione degli errori di privilegi insufficienti

Ruoli

Panoramica sulle regole di condivisione

## Risoluzione degli errori di accesso a livello di processo

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte le versioni**

AUTORIZZAZIONI UTENTE

Per visualizzare e modificare le regole di convalida:

- "Visualizza impostazione e configurazione"

  E

  "Personalizza applicazione"

Per visualizzare e definire i trigger Apex:

- "Apex autore"

Gli errori di privilegi insufficienti possono essere causati da una regola di convalida.

Per risolvere gli errori di privilegi insufficienti, normalmente è necessario stabilire se sono causati da errori nella configurazione di insiemi di autorizzazioni, profili o impostazioni di condivisione. In caso contrario, potrebbe essere necessario rivedere le regole di convalida della propria organizzazione.

1. Rivedere le proprie regole di convalida.

   È possibile che una regola di convalida impedisca all'utente di completare un'operazione, ad esempio trasferire un record caso dopo che è stato chiuso.

2. Dalle impostazioni di gestione dell'oggetto, trovare l'oggetto che si desidera controllare e scorrere verso il basso fino a Regole di convalida.
3. Verificare che l'errore non sia provocato da nessuna delle regole di convalida. Oppure, correggere la regola di convalida se l'utente può ottenere l'accesso tramite quest'ultima.

VEDERE ANCHE:

Risoluzione degli errori di privilegi insufficienti

# Domande frequenti sull'accesso ai record



## Per quale motivo un utente può avere accesso a un account?

Un utente può essere autorizzato ad accedere a un account per i seguenti motivi:

- Proprietà dei record
- Accesso implicito da un record secondario associato quale un caso, un referente o un'opportunità
- Impostazioni predefinite di condivisione valide per tutta l'organizzazione
- Gerarchia dei ruoli
- Regole di condivisione
- Condivisione manuale
- Team account o territorio

Per scoprire il motivo per cui un determinato utente dispone dell'accesso al record, fare clic sul pulsante **Condivisione** nella pagina dei dettagli dell'account per visualizzare un elenco degli utenti autorizzati all'accesso e dei motivi per cui sono autorizzati. Fare clic su **Espandi elenco** per visualizzare tutti gli utenti che possono accedere.

Gli utenti seguenti non compaiono nell'elenco anche se è possibile che siano autorizzati ad accedere:

- Tutti gli utenti, se le impostazioni predefinite di tutta l'organizzazione sono impostate su Solo lettura pubblica o Lettura/Scrittura pubblica
- Utenti del portale a volume elevato

Nota: Se il pulsante **Condivisione** non è visualizzato, è possibile che le impostazioni predefinite di tutta l'organizzazione siano state impostate su Controllato da società controllante o su Lettura pubblica. In caso contrario, la pagina Dettagli condivisione può essere visualizzata solo dal titolare del record, da un amministratore o da un utente di grado superiore al titolare nella gerarchia dei ruoli.

**Tabella 2: Indicazioni per la risoluzione dei problemi relativi all'accesso degli utenti a un record**

| Tipo di accesso | Descrizione |
| --- | --- |
| Titolare record | Il titolare del record è sempre autorizzato ad accedere ai suoi record. |
| Accesso implicito | Corrisponde alla voce "Titolare o condivisione record associato" nella colonna Motivo della pagina Dettagli condivisione. L'utente può essere autorizzato ad accedere a un record secondario di un account (opportunità, caso o referente), il che gli concede l'accesso in Lettura a quell'account. Non è possibile sovrascrivere questo accesso. Ad esempio, se l'utente può accedere a un record caso, dispone anche di accesso implicito in Lettura al record account controllante. |
| Impostazione predefinita di condivisione valida per tutta l'organizzazione | Verificare se le impostazioni predefinite per l'oggetto account sono impostate su Privato. Se lo sono, l'utente potrebbe avere ottenuto l'accesso tramite un altro dei metodi qui descritti. L'impostazione deve essere Privato se almeno uno degli utenti non deve essere in grado di vedere un record. |
| Gerarchia dei ruoli | L'utente potrebbe avere ereditato l'accesso in Lettura da un subordinato nella gerarchia dei ruoli. Per gli oggetti diversi da quelli personalizzati, questo comportamento non si può ignorare. Se l'utente che dispone di accesso è in un ramo diverso della gerarchia rispetto al titolare dell'account, controllare le regole di condivisione, i team account e il territorio account. |
| Regole di condivisione | L'utente potrebbe avere ottenuto l'accesso perché è stato incluso in una regola di condivisione pertinente. Se la regola di condivisione utilizza i gruppi pubblici (o altre categorie, ad esempio i ruoli) per concedere l'accesso, vedere se l'utente è stato incluso in uno dei propri gruppi pubblici. |
| Condivisioni manuali | L'utente potrebbe avere ottenuto l'accesso tramite il pulsante **Condivisione** del record. Le condivisioni manuali in un record possono essere create o rimosse solo dal titolare del record, da un amministratore o da un utente di grado superiore al titolare nella gerarchia dei ruoli. |
| Team account e territorio | È possibile che l'utente sia stato inserito in un team account dal titolare dell'account, da un amministratore, da un utente di grado superiore al titolare nella gerarchia dei ruoli o da un membro di un team account. Se l'organizzazione utilizza la gestione dei territori, controllare se l'utente autorizzato ad accedere ha un grado superiore a quello del titolare dell'account nella gerarchia dei territori. I responsabili godono dello stesso tipo di accesso dei loro subordinati. Inoltre, un utente membro del Gruppo A, che a sua volta è membro del Gruppo B, è autorizzato ad accedere a tutti gli account condivisi con il Gruppo B, con lo stesso livello di accesso dei membri del Gruppo B. |

VEDERE ANCHE:

Protezione dell'accesso ai dati

Risoluzione degli errori di privilegi insufficienti

# Gestione delle cartelle

Una *cartella* è un contenitore in cui vengono memorizzati rapporti, cruscotti digitali, documenti o modelli email. Le cartelle possono essere pubbliche, nascoste o condivise, oppure è possibile impostarle su sola lettura o lettura/scrittura. Il controllo dell'accesso ai contenuti può basarsi su ruoli, autorizzazioni, gruppi pubblici e tipi di licenza. È possibile rendere una cartella disponibile all'intera organizzazione oppure renderla privata in modo che l'accesso sia consentito soltanto al titolare.

- Per accedere alle cartelle dei documenti, fare clic sulla scheda **Documenti**.
- Per accedere alle cartelle dei modelli di email, da Imposta immettere *`Modelli di email`* nella casella `Ricerca veloce`, quindi selezionare **Modelli di email**.

Per creare una cartella, fare clic su **Crea nuova cartella**.

Per modificare una cartella, fare clic su **Modifica** accanto al nome della cartella. In alternativa, selezionare il nome di una cartella dall'elenco a discesa Cartelle e fare clic su **Modifica**.

Nota: i contenuti di una cartella possono essere modificati solo se il livello di accesso della cartella è impostato su lettura/scrittura. Solo gli utenti che dispongono dell'autorizzazione "Gestisci documenti pubblici" o "Gestisci modelli pubblici" possono eliminare o modificare una cartella di sola lettura. Gli utenti non possono modificare le cartelle personali o non archiviate, indipendentemente dalle autorizzazioni di cui dispongono e dalle impostazioni della cartella. Gli utenti che dispongono dell'autorizzazione "Gestisci rapporti nelle cartelle pubbliche" possono modificare tutti i rapporti nelle cartelle pubbliche ma non i rapporti nelle cartelle personali di altri utenti.

VEDERE ANCHE:

Creazione e modifica di cartelle
Eliminazione di cartelle
Inserimento di voci in cartelle

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

Le cartelle dei rapporti non sono disponibili nelle versioni: **Contact Manager Edition**, **Group Edition** e **Personal Edition**

AUTORIZZAZIONI UTENTE

Per creare, modificare ed eliminare cartelle di documenti pubblici:
- ”Gestisci documenti pubblici”

Per creare, modificare ed eliminare cartelle di modelli pubblici di email:
- "Gestisci modelli pubblici"

Per creare, modificare ed eliminare cartelle di rapporti pubblici:
- "Gestisci rapporti nelle cartelle pubbliche"

Per creare, modificare ed eliminare cartelle di cruscotti digitali pubblici:
- "Gestisci cruscotti digitali" E "Visualizza tutti i dati"

## Creazione e modifica di cartelle

EDIZIONI

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

Le cartelle dei rapporti non sono disponibili nelle versioni: **Contact Manager Edition**, **Group Edition** e **Personal Edition**

La limitazione delle cartelle di documenti non è disponibile nella versione: **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare, modificare ed eliminare cartelle di documenti pubblici:
- "Gestisci documenti pubblici"

Per creare, modificare ed eliminare cartelle di modelli pubblici di email:
- "Gestisci modelli pubblici"

Per creare, modificare ed eliminare cartelle di rapporti pubblici:
- "Gestisci rapporti nelle cartelle pubbliche"

Per creare, modificare ed eliminare cartelle di cruscotti digitali pubblici:
- "Gestisci cruscotti digitali" E "Visualizza tutti i dati"

Fare clic su **Crea nuove cartelle** o su **Modifica** nella maggior parte delle pagine in cui sono elencate le cartelle.

1. Immettere un'`Etichetta cartella`. L'etichetta viene utilizzata per indicare la cartella sulle pagine dell'interfaccia utente.
2. Se si dispone dell'autorizzazione "Personalizza applicazione", immettere un nome univoco che verrà utilizzato dall'API e dai pacchetti gestiti.
3. Scegliere un'opzione del campo `Accesso a cartelle pubbliche`. Se si desidera che gli utenti siano in grado di modificare il contenuto delle cartelle, selezionare Lettura/Scrittura. Una cartella di sola lettura può essere visibile agli utenti, ma questi non possono modificarne il contenuto.
4. Selezionare un rapporto, un cruscotto digitale o un modello non archiviato e fare clic su **Aggiungi** per memorizzarlo nella nuova cartella. Saltare questo passaggio per le cartelle di documenti.
5. Scegliere un'opzione di visibilità della cartella:
   - `Questa cartella è accessibile da tutti gli utenti, inclusi gli utenti del portale` consente l'accesso alla cartella a tutti gli utenti dell'organizzazione, compresi quelli del portale.
   - `Questa cartella è accessibile da tutti gli utenti, tranne dagli utenti del portale` consente l'accesso alla cartella a tutti gli utenti dell'organizzazione, tranne quelli del portale. Questa opzione è disponibile solo per le cartelle dei rapporti e dei cruscotti digitali nelle organizzazioni in cui è abilitato un Portale partner o un Portale Clienti. Se non si dispone di un portale, l'opzione non sarà visualizzata.
   - `Questa cartella è nascosta a tutti gli utenti` consente di configurare la cartella come privata.
   - `Questa cartella è accessibile solo ai seguenti utenti` consente di concedere l'accesso solo a un gruppo di utenti selezionati:
     a. Scegliere "Gruppi pubblici", "Ruoli", "Ruoli e subordinati", "Ruoli, subordinati interni e portale" (se i portali sono abilitati), "Territori" o "Territori e subordinati" dall'elenco a discesa `Cerca`. Le scelte disponibili variano a seconda della versione e al fatto che l'organizzazione utilizzi o meno la gestione dei territori.

        Nota: quando si condivide una cartella con un gruppo, i responsabili dei membri del gruppo non dispongono dell'accesso alla cartella se non sono essi stessi membri del gruppo.

     b. Se nell'elenco `Disponibile per la condivisione` non viene visualizzato immediatamente il valore richiesto, immettere i criteri di ricerca e fare clic su **Trova**.
     c. Selezionare il valore desiderato dall'elenco `Disponibile per la condivisione` e fare clic su **Aggiungi** per spostare il valore nell'elenco `Condivisa con`.

        Nota: per concedere agli utenti livelli di accesso più dettagliati alle cartelle di rapporti e alle cartelle di cruscotti digitali, è possibile utilizzare la condivisione ottimizzata delle cartelle. Per ulteriori informazioni, vedere Abilitazione della condivisione ottimizzata per i rapporti e i cruscotti digitali e Condivisione di una cartella dei rapporti o dei cruscotti digitali.

6. Fare clic su **Salva**.

VEDERE ANCHE:

Gestione delle cartelle

## Eliminazione di cartelle

È possibile eliminare soltanto le cartelle vuote. Prima di iniziare, rimuovere tutti i documenti, i cruscotti digitali, i modelli e i rapporti dalla cartella che si desidera eliminare.

1. Fare clic su **Modifica** accanto al nome della cartella in una pagina che contenga un elenco di cartelle. Nella scheda Rapporti, fare clic su ▾ quindi su **Modifica** nel riquadro Cartelle.
2. Fare clic su **Elimina** o su ▾ quindi su **Elimina**.
3. Fare clic su **OK** per confermare.

VEDERE ANCHE:

Gestione delle cartelle

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

Le cartelle dei rapporti non sono disponibili nelle versioni: **Contact Manager Edition**, **Group Edition** e **Personal Edition**

AUTORIZZAZIONI UTENTE

Per creare, modificare ed eliminare cartelle di documenti pubblici:

- "Gestisci documenti pubblici"

Per creare, modificare ed eliminare cartelle di modelli pubblici di email:

- "Gestisci modelli pubblici"

Per creare, modificare ed eliminare cartelle di rapporti pubblici:

- "Gestisci rapporti nelle cartelle pubbliche"

Per creare, modificare ed eliminare cartelle di cruscotti digitali pubblici:

- "Gestisci cruscotti digitali" E "Visualizza tutti i dati"

# Inserimento di voci in cartelle

Per spostare un documento, un cruscotto digitale, un rapporto o un modello di email in una cartella diversa:

1. Selezionare la voce che si desidera archiviare in una cartella.
2. Fare clic su **Modifica proprietà**.
3. Scegliere un'altra cartella.
4. Fare clic su **Salva**.

Analogamente alle cartelle rapporti, che contengono solo rapporti, e alle cartelle di modelli di email, che contengono solo modelli di email, le cartelle documenti possono contenere solo documenti. Per archiviare un allegato in una cartella di documenti, salvarlo sul computer e caricarlo nella libreria dei documenti.

Nota: i modelli di email utilizzati da Web a caso, Web a lead, regole di assegnazione o regole di inoltro al livello superiore devono essere contrassegnati come "Disponibile all'uso".

VEDERE ANCHE:

Gestione delle cartelle

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

Le cartelle dei rapporti non sono disponibili nelle versioni: **Contact Manager Edition**, **Group Edition** e **Personal Edition**

AUTORIZZAZIONI UTENTE

Per creare, modificare ed eliminare cartelle di documenti pubblici:

- "Gestisci documenti pubblici"

Per creare, modificare ed eliminare cartelle di modelli pubblici di email:

- "Gestisci modelli pubblici"

Per creare, modificare ed eliminare cartelle di rapporti pubblici:

- "Gestisci rapporti nelle cartelle pubbliche"

Per creare, modificare ed eliminare cartelle di cruscotti digitali pubblici:

- "Gestisci cruscotti digitali" E "Visualizza tutti i dati"

# Importazione dei dati

## Panoramica sull'importazione

È possibile importare fino a 50.000 record in Salesforce da una fonte dati esistente.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

I tipi di oggetti che è possibile importare sono determinati dalla versione (Edition) utilizzata.

Importante: Salesforce ha sostituito le singole procedure di importazione guidata per account, referenti e altri oggetti con una procedura unificata di Importazione guidata dati (le singole procedure di importazione guidata si aprono in piccole finestre popup, mentre l'importazione unificata si apre in un browser di dimensioni normali con dataimporter.app alla fine dell'URL). Per iniziare a utilizzare la procedura unificata, da Imposta, immettere *Importazione guidata dati* nella casella `Ricerca veloce`, quindi selezionare **Importazione guidata dati**. (le opzioni visualizzate dipendono dalle autorizzazioni di cui si dispone).

È possibile importare i dati da ACT!, da Outlook e da qualsiasi programma che salvi i dati nel formato delimitato da virgole (.csv), come Excel o GoldMine.

Nota: se le virgole non sono appropriate per le proprie impostazioni internazionali, utilizzare la tabulazione o un altro delimitatore.

Il numero di record che è possibile importare dipende dalle autorizzazioni dell'utente e dal tipo di dati che si stanno importando. È possibile importare tutti i record consentiti, a condizione che non si superino i limiti di memoria dati complessivi previsti per l'organizzazione

**Quali record possono essere importati?**

| Tipo di record | Limite record di importazione | Utenti con accesso | Panoramica |
|---|---|---|---|
| Account aziendali e referenti di cui si è titolari | 500 per volta | Tutti gli utenti | Quali elementi vengono importati per gli account aziendali e i referenti? |
| Account aziendali e referenti di cui sono titolari altri utenti | 50.000 per volta | Amministratori;<br>Gli utenti che dispongono dell'autorizzazione "Modifica tutti i dati" | Quali elementi vengono importati per gli account aziendali e i referenti? |
| Account personali di cui si è titolari | 50.000 per volta | Tutti gli utenti | Quali elementi vengono importati per gli account personali? |
| Account personali di cui sono titolari altri utenti | 50.000 per volta | Amministratori;<br>Utenti dotati di autorizzazione "Importa account personali" | Quali elementi vengono importati per gli account personali? |
| Lead | 50.000 per volta | Amministratori;<br>Utenti con autorizzazione "Lettura", "Crea" e "Modifica" sui lead e con autorizzazione "Importa lead" | Cosa viene importato per i lead? |

**Quali record possono essere importati?**

| Tipo di record | Limite record di importazione | Utenti con accesso | Panoramica |
|---|---|---|---|
| Membri di una campagna | 50.000 per l'importazione di lead come nuovi membri della campagna e l'aggiornamento dello stato di membri campagna esistenti. | Amministratori;<br>Gli utenti marketing o gli utenti che dispongono delle autorizzazioni "Importa lead" e "Modifica" per le campagne possono importare i lead come membri campagna. Per utilizzare Aggiornamento guidato campagna per rendere lead e referenti esistenti membri della campagna, è necessario che gli utenti dispongano inoltre dell'autorizzazione "Lettura". | Cosa viene importato per i membri campagna? |
| Oggetti personalizzati | 50.000 per volta | Amministratori;<br>Gli utenti che dispongono dell'autorizzazione "Modifica tutti i dati" | Cosa viene importato per gli oggetti personalizzati? |
| Soluzioni | 50.000 per volta | Amministratori;<br>Utenti dotati di autorizzazione "Importa soluzioni" | Cosa viene importato per le soluzioni? |
| Asset<br>Casi<br>Campagne<br>Contratti<br>Documenti<br>Opportunità<br>Prodotti | Questi record non possono essere importati mediante le importazioni guidate. | | |

Per informazioni sull'accessibilità dei campi e sulle modalità di importazione dei valori dei diversi tipi di campi, vedere Note sull'importazione di dati a pagina 348.

Nota: I membri dei gruppi relazione non possono essere importati.

VEDERE ANCHE:

Importazione guidata dati

Decisione del metodo di importazione ed esportazione dei dati

Annullamento di un'importazione

# Decisione del metodo di importazione ed esportazione dei dati

Di seguito sono descritte le opzioni di importazione ed esportazione dei dati in e da Salesforce.

| Strumento | Versioni supportate | Numero di record che è possibile importare o esportare | Importazione | Esportazione | Interno o esterno a Salesforce | Informazioni aggiuntive |
| --- | --- | --- | --- | --- | --- | --- |
| Importazione guidata dati (unificata) | Tutte le versioni tranne Database.com Edition | Fino a 50.000 | Sì | No | Interno | Procedura guidata del browser che effettua l'importazione degli account, referenti, lead, soluzioni e oggetti personalizzati dell'organizzazione. Scopri altre informazioni. |
| Data Loader | Enterprise Edition, Unlimited Edition, Performance Edition, Developer Edition e Database.com Edition | Tra 5.000 e 5 milioni | Sì | Sì | Esterno | Data Loader è un'applicazione per l'importazione o l'esportazione in massa di dati. È possibile utilizzarlo per inserire, aggiornare, eliminare o esportare record di Salesforce. Scopri altre informazioni. |
| Procedura guidata di importazione di account personali e referenti | Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition e Developer Edition | Fino a 500 record per un singolo utente<br>Fino a 50.000 record per più utenti | Sì | No | Interno | Procedura guidata incorporata nel browser che consente di importare referenti e account personali da varie fonti di dati, come Act!™, Gmail™ e Outlook®. |
| Esportazione dati | Esportazione settimanale | Nessun limite | No | Sì | Interno | Una procedura guidata del browser che esporta i dati in file |

| Strumento | Versioni supportate | Numero di record che è possibile importare o esportare | Importazione | Esportazione | Interno o esterno a Salesforce | Informazioni aggiuntive |
| --- | --- | --- | --- | --- | --- | --- |
| | disponibile nelle versioni Enterprise Edition, Unlimited Edition e Performance Edition. Esportazione mensile disponibile in tutte le versioni tranne Database.com. | | | | | .zip con dimensioni massime di 128 MB su base mensile o settimanale. Scopri altre informazioni. |

Salesforce fornisce delle API che integrano i dati con Salesforce. Per decidere qual è l'API più adatta, verificare qual è il numero di record da importare o esportare e quali sono le tecnologie di integrazione necessarie.

| API | Versioni supportate | Numero di record che è possibile importare o esportare | Importazione | Esportazione | Questa API consente |
| --- | --- | --- | --- | --- | --- |
| API REST | Developer Edition, Enterprise Edition, Unlimited Edition, Performance Edition e Database.com Edition | 200 o meno | Sì | Sì | Accedere agli oggetti dell'organizzazione utilizzando l'API REST. |
| API SOAP | Developer Edition, Enterprise Edition, Unlimited Edition, Performance Edition e Database.com Edition | 200 o meno | Sì | Sì | Integrare i dati dell'organizzazione con altre applicazioni utilizzando l'API SOAP. |

| API | Versioni supportate | Numero di record che è possibile importare o esportare | Importazione | Esportazione | Questa API consente |
| --- | --- | --- | --- | --- | --- |
| API in blocco | Developer Edition, Enterprise Edition, Unlimited Edition, Performance Edition e Database.com Edition | Un milione o più | Sì | Sì | Caricare o eliminare grandi quantità di record utilizzando l'API in blocco. |

VEDERE ANCHE:

Importazione guidata dati

Panoramica sull'importazione

## Quali elementi vengono importati per gli account aziendali e i referenti?

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

Importazione organizzazione non disponibile nella versione: **Personal Edition**, **Database.com Edition**

Le importazioni guidate per referenti e account aziendali consentono di individuare la corrispondenza tra record in diversi modi evitando così la creazione di duplicati. Per i referenti è possibile individuare le corrispondenze in base a ID Salesforce, nome o email. La corrispondenza tra gli account aziendali può essere individuata in base all'ID Salesforce o a nome e sito. La corrispondenza in base all'ID Salesforce agisce sia sui referenti sia sugli account aziendali; se si esegue la corrispondenza di uno in base all'ID Salesforce, anche l'altro verrà individuato in base a questo criterio.

### Corrispondenza per nome e sito

Se si decide di far corrispondere i referenti per nome e gli account aziendali per nome e sito (ossia le opzioni consigliate), le procedure guidate di importazione creano automaticamente un account aziendale per ogni specifico nome e sito di account aziendale nel file di importazione. Viene inoltre creato un referente separato per ogni nome di referente elencato nel file. I referenti vengono quindi associati agli account aziendali appropriati.

Se nel sistema esiste già l'account aziendale o il referente e si dispone di accesso in lettura/scrittura al record, i dati importati verranno aggiunti ai dati esistenti in Salesforce. Inoltre, se un nome di account aziendale o di referente nel file di importazione è simile a un nome di account aziendale o di referente esistente, i dati importati vengono aggiunti ai dati esistenti in Salesforce.

### Corrispondenza per ID Salesforce

È anche possibile decidere di individuare le corrispondenze tra referenti e tra account aziendali in base all'ID Salesforce. Se si sceglie questa opzione, l'ID Salesforce sarà il criterio per l'eliminazione di duplicati. In altre parole, se si effettua la corrispondenza per ID e in un record del file di origine è presente lo stesso ID di un record in Salesforce, tale record verrà aggiornato in Salesforce. Si noti che gli ID di record fanno distinzione tra maiuscole e minuscole, pertanto devono corrispondere perfettamente.

### Sovrascrittura di valori di account esistenti

Non viene sovrascritto alcun campo di account aziendale esistente se non si seleziona la casella di controllo `Sovrascrivere valori di account esistenti` nella procedura guidata. Quando questa casella di controllo è selezionata è possibile inserire o aggiornare i campi degli account aziendali esistenti con nuovi dati. Non è tuttavia possibile utilizzare tale casella di controllo per aggiornare con valori vuoti i dati dei campi esistenti. Quando questa casella di controllo è deselezionata, vengono aggiornati i campi di account aziendali vuoti lasciando inalterati i campi con dati esistenti.

Se non si dispone di accesso in lettura/scrittura a un account aziendale o referente esistente, viene creato un nuovo account aziendale o referente di cui si diventa titolari. Inoltre, vengono creati nuovi account aziendali e referenti in base a specifici campi nel file di importazione.

Nelle organizzazioni che utilizzano le versioni Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition e Developer Edition è inoltre possibile importare nuove note relative ad account aziendali e referenti. Le note che sono duplicati esatti di note referente o account aziendali già esistenti non vengono importate.

VEDERE ANCHE:

Importazione guidata dati
Importazione di referenti personali da Outlook o ACT!
Importazione referenti personali da altre fonti
Decisione del metodo di importazione ed esportazione dei dati
Panoramica sull'importazione

## Quali elementi vengono importati per gli account personali?

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

L'importazione di account personali è disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Importante: Salesforce ha sostituito le singole procedure di importazione guidata per account, referenti e altri oggetti con una procedura unificata di Importazione guidata dati (le singole procedure di importazione guidata si aprono in piccole finestre popup, mentre l'importazione unificata si apre in un browser di dimensioni normali con dataimporter.app alla fine dell'URL). Per iniziare a utilizzare la procedura unificata, da Imposta, immettere *`Importazione guidata dati`* nella casella `Ricerca veloce`, quindi selezionare **Importazione guidata dati**. (le opzioni visualizzate dipendono dalle autorizzazioni di cui si dispone).

L'importazione guidata per gli account personali consente di evitare la creazione di record duplicati individuando le corrispondenze tra i record in base a uno dei seguenti campi: `Nome account`, `ID Salesforce` o `Email`. Includere nel file di importazione una colonna per il campo da utilizzare per l'individuazione della corrispondenza tra record.

Nota: è possibile che l'amministratore abbia rinominato "account personale". In questo caso la procedura guidata di importazione farà riferimento al nuovo nome.

### Corrispondenza per nome

Quando si seleziona questa opzione, l'importazione guidata rileverà i record esistenti in Salesforce che hanno lo stesso nome. In questo tipo di corrispondenza non è rilevante la distinzione tra maiuscole e minuscole. I nomi che iniziano con una lettera maiuscola, ad esempio, corrisponderanno allo stesso nome che inizia con la lettera minuscola. Se necessario, analizzare e standardizzare i nomi degli oggetti personalizzati prima di eseguire l'importazione per evitare corrispondenze indesiderate.

## Corrispondenza per ID Salesforce

Un ID Salesforce è una stringa generata dal sistema con distinzione tra maiuscole e minuscole, composta da 15 o 18 lettere e numeri, che identifica in modo univoco ogni record di Salesforce. Quando si seleziona questa opzione, l'importazione guidata rileverà i record esistenti in Salesforce associati allo stesso ID Salesforce. Per gli ID Salesforce è rilevante la distinzione tra maiuscole e minuscole e la corrispondenza deve essere esatta. Gli ID Salesforce possono essere ottenuti mediante l'esecuzione di rapporti che includono il campo ID del record.

## Corrispondenza per email

Con questa opzione gli account personali del file di importazione vengono fatti corrispondere agli account personali esistenti in Salesforce in base al valore esatto del campo `Email`.

## Corrispondenza per ID esterno

Un ID esterno è un campo personalizzato che possiede l'attributo "ID esterno", ovvero contiene identificatori univoci di record di un sistema esterno a Salesforce. Quando si seleziona questa opzione, l'importazione guidata rileverà i record esistenti in Salesforce che sono associati allo stesso ID esterno. Per questa operazione non è rilevante la distinzione tra maiuscole e minuscole, ossia "ABC" corrisponde ad "abc". Esiste però un'eccezione: se il campo personalizzato possiede l'attributo "Univoco" e se è selezionata l'opzione per la distinzione tra maiuscole e minuscole, le lettere maiuscole e minuscole non saranno considerate identiche.

Se necessario, analizzare e standardizzare i valori di ID esterno prima di eseguire l'importazione per evitare corrispondenze indesiderate.

Quando si ricercano le corrispondenze per ID esterno, se l'importazione guidata individua record duplicati, nel messaggio di conferma vengono riportati solo i primi tre record duplicati.

Nota: questa procedura può essere eseguita solo con i campi di account personalizzati dotati dell'attributo "ID esterno". Mentre tutti i campi referenti personalizzati sono disponibili nei layout di pagina degli account personali, i campi referenti personalizzati che possiedono l'attributo "ID esterno" non sono disponibili come campi corrispondenti durante l'importazione di account personali.

## Ignorare o aggiornare i record corrispondenti

Quando l'importazione guidata rileva record esistenti in Salesforce che corrispondono in base al campo selezionato, è possibile effettuare una delle seguenti operazioni:

- **Non aggiornare i record esistenti e inserire solo i nuovi record** - Se nel file sono presenti record nuovi non corrispondenti ad alcun record esistente, inserirli in Salesforce. Inoltre, i record che corrispondono ad un record esistente vengono ignorati e non viene effettuata alcuna operazione sui record esistenti.
- **Aggiornare record esistenti e non inserire nuovi record** - Se nel file sono presenti record che corrispondono a un record esistente, aggiornare il record esistente. Inoltre, i record che non corrispondono ad un record esistente vengono ignorati e non vengono inseriti come nuovi record.

- **Aggiornare i record esistenti e inserire nuovi record** - Se nel file sono presenti record nuovi non corrispondenti ad alcun record esistente, inserirli in Salesforce. Inoltre, se nel file sono presenti record corrispondenti ad un record esistente, quest'ultimo viene aggiornato.

VEDERE ANCHE:

Importazione guidata dati

Importazione degli account personali

Importa account personali dell'organizzazione

Decisione del metodo di importazione ed esportazione dei dati

Panoramica sull'importazione

## Cosa viene importato per i lead?

È possibile importare dati nei campi standard dei lead e in qualsiasi campo lead personalizzato, anche se un particolare campo è nascosto o di sola lettura nel layout di pagina o nelle impostazioni di protezione a livello di campo per i lead.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

### Importazione di lead con tipi corrispondenti

È possibile scegliere se effettuare la corrispondenza tra i lead del file di importazione e i lead esistenti in Salesforce. Le corrispondenze dei lead possono essere individuate in base ai seguenti tipi: ID Salesforce, nome o email. La scelta di un tipo di corrispondenza consente di impostare i criteri per evitare lead duplicati. Ad esempio, se si effettua la corrispondenza per email e in un lead del file di origine è presente lo stesso indirizzo email di un lead in Salesforce, tale lead verrà aggiornato in Salesforce. Se non si effettua la corrispondenza per email e in un lead del file di origine è presente lo stesso indirizzo email di un lead in Salesforce, verrà creato un nuovo lead.

Non viene sovrascritto alcun campo di lead esistente se non si seleziona la casella di controllo `Sovrascrivere valori di lead esistenti` nella procedura guidata. Quando questa casella di controllo è selezionata è possibile inserire o aggiornare i campi dei lead esistenti con nuovi dati. Non è tuttavia possibile utilizzare tale casella di controllo per aggiornare con valori vuoti i dati dei campi esistenti. Quando questa casella di controllo è deselezionata, i campi di lead vuoti vengono aggiornati lasciando inalterati i campi con dati esistenti.

### Importazione di lead senza tipi corrispondenti

Se si sceglie il tipo di corrispondenza "Nessuno" nella procedura Importazione guidata dati, per ogni lead nel file di importazione la procedura guidata crea un nuovo lead in Salesforce. È possibile unire i lead dopo la loro importazione.

VEDERE ANCHE:

Importazione guidata dati

Decisione del metodo di importazione ed esportazione dei dati

## Cosa viene importato per i membri campagna?

- **Importazione guidata dati** - Per ogni lead presente nel file di importazione, questa procedura importa il lead, lo associa a una campagna e inserisce il valore `Stato membro` per il lead in quella campagna. È possibile importare dati nei campi standard dei lead e in qualsiasi campo lead personalizzato, anche se un particolare campo è nascosto o di sola lettura nel layout di pagina o nelle impostazioni di protezione a livello di campo per i lead. Se il file di importazione contiene lead duplicati, questi ultimi non vengono uniti durante la procedura guidata. Inoltre, se uno qualsiasi dei lead importati corrisponde a un lead esistente, la procedura di importazione non unisce i dati duplicati in un unico lead.
- **Aggiornamento guidato campagna** - Per ogni referente o lead nel file di importazione, questa procedura aggiorna solo il valore di `Stato membro` del referente o lead corrispondente in Salesforce. Non è possibile aggiungere nuovi lead o referenti, né aggiornare altri campi dei record di lead o referenti esistenti.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

VEDERE ANCHE:

Importazione guidata dati

Decisione del metodo di importazione ed esportazione dei dati

## Cosa viene importato per gli oggetti personalizzati?

La procedura Importazione guidata dati per gli oggetti personalizzati consente di evitare la creazione di record duplicati individuando le corrispondenze tra i record in base a uno dei seguenti campi: nome oggetto personalizzato, ID Salesforce o ID esterno. Nel file di importazione, includere una colonna per il campo da utilizzare per la corrispondenza tra i record.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Importazione oggetti personalizzati disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per importare oggetti personalizzati:
- "Modifica tutti i dati"

### Corrispondenza per nome

Quando si seleziona questa opzione, l'importazione guidata rileverà i record esistenti in Salesforce che hanno lo stesso nome. In questo tipo di corrispondenza non è rilevante la distinzione tra maiuscole e minuscole. I nomi che iniziano con una lettera maiuscola, ad esempio, corrisponderanno allo stesso nome che inizia con la lettera minuscola. Se necessario, analizzare e standardizzare i nomi degli oggetti personalizzati prima di eseguire l'importazione per evitare corrispondenze indesiderate.

### Corrispondenza per ID Salesforce

Un ID Salesforce è una stringa generata dal sistema con distinzione tra maiuscole e minuscole, composta da 15 o 18 lettere e numeri, che identifica in modo univoco ogni record di Salesforce. Quando si seleziona questa opzione, l'importazione guidata rileverà i record esistenti in Salesforce associati allo stesso ID Salesforce. Per gli ID Salesforce è rilevante la distinzione tra maiuscole e minuscole e la corrispondenza deve essere esatta. Gli ID Salesforce possono essere ottenuti mediante l'esecuzione di rapporti che includono il campo ID del record.

### Corrispondenza per ID esterno

Un ID esterno è un campo personalizzato che possiede l'attributo "ID esterno", ovvero contiene identificatori univoci di record di un sistema esterno a Salesforce. Quando si seleziona questa opzione, l'importazione guidata rileverà i record esistenti in Salesforce che sono associati allo stesso ID esterno. Per questa operazione non è rilevante la distinzione tra maiuscole e minuscole, ossia "ABC" corrisponde

ad "abc". Esiste però un'eccezione: se il campo personalizzato possiede l'attributo "Univoco" e se è selezionata l'opzione per la distinzione tra maiuscole e minuscole, le lettere maiuscole e minuscole non saranno considerate identiche.

Se necessario, analizzare e standardizzare i valori di ID esterno prima di eseguire l'importazione per evitare corrispondenze indesiderate.

Quando si ricercano le corrispondenze per ID esterno, se l'importazione guidata individua record duplicati, nel messaggio di conferma vengono riportati solo i primi tre record duplicati.

### Ignorare o aggiornare i record corrispondenti

Quando l'importazione guidata rileva record esistenti in Salesforce che corrispondono in base al campo selezionato, è possibile effettuare una delle seguenti operazioni:

- **Non aggiornare i record esistenti e inserire solo i nuovi record** - Se nel file sono presenti record nuovi non corrispondenti ad alcun record esistente, inserirli in Salesforce. Inoltre, i record che corrispondono ad un record esistente vengono ignorati e non viene effettuata alcuna operazione sui record esistenti.
- **Aggiornare record esistenti e non inserire nuovi record** - Se nel file sono presenti record che corrispondono a un record esistente, aggiornare il record esistente. Inoltre, i record che non corrispondono ad un record esistente vengono ignorati e non vengono inseriti come nuovi record.
- **Aggiornare i record esistenti e inserire nuovi record** - Se nel file sono presenti record nuovi non corrispondenti ad alcun record esistente, inserirli in Salesforce. Inoltre, se nel file sono presenti record corrispondenti ad un record esistente, quest'ultimo viene aggiornato.

Nota: gli oggetti personalizzati con due relazioni record principale-record dettaglio non possono essere importati mediante la procedura guidata.

VEDERE ANCHE:

Importazione guidata dati

Decisione del metodo di importazione ed esportazione dei dati

## Cosa viene importato per le soluzioni?

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per importare le soluzioni:
- "Importa soluzioni"

La procedura Importazione guidata dati consente di evitare la creazione di record duplicati individuando le corrispondenze tra i record in base a uno dei seguenti campi: titolo soluzione, ID Salesforce o ID esterno. Nel file di importazione, includere una colonna per il campo da utilizzare per la corrispondenza tra i record.

### Corrispondenza per titolo soluzione

Quando si seleziona questa opzione, l'importazione guidata rileverà le soluzioni esistenti in Salesforce che hanno lo stesso titolo. In questo tipo di corrispondenza non è rilevante la distinzione tra maiuscole e minuscole. I titoli che iniziano con una lettera maiuscola, ad esempio, corrisponderanno allo stesso titolo che inizia con la lettera minuscola. Se necessario, analizzare e standardizzare i titoli delle soluzioni prima di eseguire l'importazione per evitare corrispondenze indesiderate.

### Corrispondenza per ID Salesforce

Un ID Salesforce è una stringa generata dal sistema con distinzione tra maiuscole e minuscole, composta da 15 o 18 lettere e numeri, che identifica in modo univoco ogni record di Salesforce. Quando si seleziona questa opzione, l'importazione guidata rileverà i record esistenti in Salesforce

associati allo stesso ID Salesforce. Per gli ID Salesforce è rilevante la distinzione tra maiuscole e minuscole e la corrispondenza deve essere esatta. Gli ID Salesforce possono essere ottenuti mediante l'esecuzione di rapporti che includono il campo ID del record.

### Corrispondenza per ID esterno

Un ID esterno è un campo personalizzato che possiede l'attributo "ID esterno", ovvero contiene identificatori univoci di record di un sistema esterno a Salesforce. Quando si seleziona questa opzione, l'importazione guidata rileverà i record esistenti in Salesforce che sono associati allo stesso ID esterno. Per questa operazione non è rilevante la distinzione tra maiuscole e minuscole, ossia "ABC" corrisponde ad "abc". Esiste però un'eccezione: se il campo personalizzato possiede l'attributo "Univoco" e se è selezionata l'opzione per la distinzione tra maiuscole e minuscole, le lettere maiuscole e minuscole non saranno considerate identiche.

Se necessario, analizzare e standardizzare i valori di ID esterno prima di eseguire l'importazione per evitare corrispondenze indesiderate.

Quando si ricercano le corrispondenze per ID esterno, se l'importazione guidata individua record duplicati, nel messaggio di conferma vengono riportati solo i primi tre record duplicati.

### Ignorare o aggiornare i record corrispondenti

Quando l'importazione guidata rileva record esistenti in Salesforce che corrispondono in base al campo selezionato, è possibile effettuare una delle seguenti operazioni:

- **Non aggiornare i record esistenti e inserire solo i nuovi record** - Se nel file sono presenti record nuovi non corrispondenti ad alcun record esistente, inserirli in Salesforce. Inoltre, i record che corrispondono ad un record esistente vengono ignorati e non viene effettuata alcuna operazione sui record esistenti.
- **Aggiornare record esistenti e non inserire nuovi record** - Se nel file sono presenti record che corrispondono a un record esistente, aggiornare il record esistente. Inoltre, i record che non corrispondono ad un record esistente vengono ignorati e non vengono inseriti come nuovi record.
- **Aggiornare i record esistenti e inserire nuovi record** - Se nel file sono presenti record nuovi non corrispondenti ad alcun record esistente, inserirli in Salesforce. Inoltre, se nel file sono presenti record corrispondenti ad un record esistente, quest'ultimo viene aggiornato.

VEDERE ANCHE:

Importazione guidata dati

Decisione del metodo di importazione ed esportazione dei dati

## Note sull'importazione di dati

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

I tipi di oggetti che è possibile importare sono determinati dalla versione (Edition) utilizzata.

- **Accessibilità campo** - Nelle importazioni guidate di account e lead a livello di organizzazione, è possibile importare dati in qualsiasi campo standard o personalizzato anche se nel layout di pagina o nelle impostazioni della protezione a livello di campo tale campo è contrassegnato come nascosto o di sola lettura. Nell'importazione guidata dei referenti personali, è possibile importare dati solo nei campi che sono modificabili dall'utente nel layout di pagina o nelle impostazioni di protezione a livello di campo.

  La protezione a livello di campo è disponibile solo nelle versioni Enterprise Edition, Unlimited Edition, Performance Edition e Developer Edition.

- **Nuovi valori per elenchi di selezione ed elenchi di selezione a selezione multipla** - Se il file da importare contiene dati da visualizzare in elenchi di selezione o elenchi di selezione a selezione multipla, la procedura guidata informa l'utente quando si tenta di importare un nuovo valore di elenco di selezione che non corrisponde ad alcun valore di elenco di selezione valido. Se si ignora l'avviso, il nuovo valore viene aggiunto automaticamente

al record importato. L'amministratore può successivamente modificare il campo per aggiungervi i valori necessari. Tenere presente che le importazioni guidate non consentono di importare più di 100 nuovi valori di elenco di selezione o di elenco di selezione a selezione multipla per qualsiasi campo nel corso di un'unica importazione.

Se l'organizzazione utilizza l'Area di lavoro traduzione, le importazioni guidate cercano i valori tradotti corrispondenti prima di creare nuovi valori di elenco di selezione non attivi.

- **Elenchi di selezione a selezione multipla** - Per importare più valori in un elenco di selezione a selezione multipla, è necessario separare i valori con un punto e virgola nel file da importare.

  In un campo elenco di selezione a selezione multipla è possibile importare fino a 100 valori alla volta. Se il file da importare contiene più di 100 valori per un record qualsiasi, l'importazione guidata lascia vuoto il campo in tale record.

- **Caselle di controllo** - Per importare dati in un campo casella di controllo, utilizzare 1 per indicare valori selezionati e 0 per indicare valori deselezionati.
- **Valori predefiniti** - Per i campi elenco di selezione, elenco di selezione a selezione multipla e casella di controllo, se nell'importazione guidata non si effettua alcuna mappatura, nel nuovo record o nel record aggiornato viene inserito automaticamente il valore predefinito, se disponibile.
- **Campi data/ora** — Verificare che il formato dei campi data/ora da importare corrisponda alla loro visualizzazione in Salesforce in base alle impostazioni internazionali dell'utente.
- **Campi formula** - I campi formula non possono accettare dati importati, poiché sono di sola lettura.
- **Regole di convalida dei campi**—Salesforce esegue regole di convalida sui record prima che vengano importati. I record che non superano la convalida non vengono importati. Se le regole di convalida influiscono sui record che si stanno importando, è possibile disattivarle prima di eseguire l'importazione.
- **Campi universalmente obbligatori**—È necessario includere i campi universalmente obbligatori nei file di importazione, altrimenti l'importazione non andrà a buon fine.

VEDERE ANCHE:

Importazione guidata dati

Decisione del metodo di importazione ed esportazione dei dati

Panoramica sull'importazione

# Importazione di più valute

Se nell'organizzazione è impostato l'utilizzo di più valute, è possibile importare importi in valute diverse.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

## Importazione di account personali e referenti

Per le importazioni personali tutti gli ammontare nei nuovi account e referenti sono importati nella valuta personale. Quando l'importazione aggiorna gli importi nei record esistenti, gli importi nel file vengono convertiti dalla valuta personale a quella dell'account o del referente.

Si supponga ad esempio che la valuta personale sia il dollaro statunitense e che il file di importazione contenga il valore 100 come reddito annuale di un account esistente con l'euro come `Valuta account`. Il nuovo valore `Reddito annuale` dell'account è EUR 92, presumendo un tasso di conversione pari a 0,92 e "EUR" come codice valuta per l'euro.

### Importazione dell'organizzazione

Quando si importano account, referenti, oggetti personalizzati, lead o soluzioni per la propria organizzazione, è possibile specificare il tipo di valuta per i campi Ammontare utilizzando la colonna `Codice ISO valuta` nel file di importazione. Vengono applicate le seguenti regole.

- **Inserimento di codici valuta** - Inserire il codice di una valuta nella colonna `Codice ISO valuta` nel file di importazione. I codici delle valute sono codici formati da tre lettere che rispettano uno standard internazionale. Ad esempio, USD è il codice valuta per il dollaro statunitense. Da Imposta, immettere *`Gestisci valute`* nella casella `Ricerca veloce`, quindi selezionare **Gestisci valute** per visualizzare un elenco di codici validi per l'organizzazione.
- **Utilizzo di una valuta per account e referenti** - Se si importano account e referenti, la colonna `Codice ISO valuta` è valida sia per un account che per il referente a esso associato. Non è possibile specificare valute diverse per account e referenti associati.
- **Aggiornamento del codice valuta** - Quando si aggiorna il codice valuta ma non gli importi in valuta per gli account e referenti esistenti, l'importo non viene convertito nel numero corrispondente nella nuova valuta.
- **Inserimento di valute non attive** - Se si inserisce una valuta non attiva nel file di importazione, viene utilizzata la valuta personale. Tuttavia gli importi non vengono modificati. Se ad esempio nel file è contenuto il valore AUD 100 per 100 dollari australiani ma AUD è una valuta non attiva per l'organizzazione, il valore verrà importato come USD 100, presumendo che la valuta personale sia il dollaro statunitense.
- **Omissione della colonna Codice ISO valuta** - Quando si creano nuovi record tramite importazione, se non si utilizza la colonna `Codice ISO valuta` o non si esegue la mappatura, verrà utilizzata la valuta personale. Se ad esempio il file presenta 100 e la valuta personale è il dollaro statunitense (codice valuta = USD), questo valore viene importato come USD 100.

  Quando si aggiornano record esistenti tramite importazione, se non si utilizza la colonna `Codice ISO valuta` o non si esegue la mappatura, gli importi vengono considerati associati alla valuta del record. Se ad esempio nel file è presente il valore 100 per un record con valuta EUR (il codice di valuta per gli euro), esso viene interpretato come EUR 100.

VEDERE ANCHE:

Importazione guidata dati

## Creazione di file di esportazione per procedure di importazione

Prima di importare i dati in Salesforce, utilizzare il software esistente per creare un file di esportazione dati.

Un file di esportazione contiene tutte le informazioni che si desidera importare.

Il file di esportazione può contenere una combinazione di nuovi record e di aggiornamenti di record esistenti. Sarà necessario scegliere in che modo vengono individuate le corrispondenze tra i record per evitare duplicazioni. Ad esempio, si può decidere che la corrispondenza di account e referenti venga effettuata in base al nome o all'indirizzo email. Se si sceglie la corrispondenza in base all'indirizzo email, il referente già presente in Salesforce verrà aggiornato se un record presente nei dati importati ha lo stesso indirizzo email. Tuttavia, se i record hanno lo stesso nome ma indirizzi email diversi, i record resteranno separati.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

1. Utilizzare il software esistente per creare un file di esportazione dati.
   - Esportazione da ACT!
   - Esportazione da LinkedIn®
   - Esportazione da Outlook
   - Esportazione da GoldMine 4.0

- Esportazione da GoldMine 5.0
- Esportazione da Palm Desktop
- Esportazione da altre fonti di dati
- Esportazione da Salesforce

2. Rivedere i dati che verranno importati per verificare che siano più aggiornati di quelli già presenti in Salesforce. I dati di Salesforce saranno sostituiti con i dati del file di importazione anche se questi non sono aggiornati.
3. Confrontare i campi di dati con i campi di Salesforce in cui è possibile effettuare l'importazione e verificare che i dati verranno mappati ai campi Salesforce appropriati. Vedere Preparazione dei dati per l'importazione a pagina 356.
4. Se si è l'amministratore e si sta eseguendo l'importazione per più utenti, combinare i dati di esportazione da più fonti in un unico file delimitato da virgole (.csv) utilizzando Excel.

   Nota: Quando si importano record per più utenti, il file di esportazione deve includere un campo `Titolare record` per tutti i nuovi record che devono contenere i nomi utente completi o i nomi e cognomi degli utenti esistenti e attivi. I titolari dei record esistenti non verranno modificati; i nuovi record verranno assegnati all'utente elencato nel campo `Titolare record`. Ad esempio, i record dell'organizzazione di cui dovrebbe essere titolare Mario Rossi devono contenere il suo nome utente (ad esempio "mrossi@acme.com") oppure il nome e cognome (ad esempio, "Mario Rossi" oppure "Rossi Mario" per le impostazioni internazionali asiatiche). Per le importazioni di lead, è anche possibile specificare il nome di un'area di attesa dei lead.

   Quando si importano i lead, è possibile in alternativa utilizzare una regola di assegnazione dei lead per specificare i titolari dei dati importati, invece di utilizzare un campo `Titolare record`.

## Esportazione da ACT!

ACT! consente di esportare dati di referenti in un formato di testo delimitato che può successivamente essere importato. Per esportare dati di referenti da ACT! (versioni 4.0 o 2000):

1. Avviare ACT! e aprire il database.
2. Selezionare **File** > **Data Exchange** > **Export...**.
3. Selezionare il tipo di file **Text-Delimited**.
4. Scegliere un nome file e un percorso per i dati esportati, quindi fare clic su **Next**
5. Selezionare **Contact records only**.
6. Fare clic sul pulsante **Options...**.
7. Selezionare **Comma** come carattere separatore di campo.

   Nota: se le virgole non sono appropriate per le proprie impostazioni internazionali, utilizzare la tabulazione o un altro delimitatore.

8. Selezionare **Yes, export field names** e fare clic su **OK**.
9. Fare clic su **Avanti**.
10. Selezionare **All Records** quindi fare clic su **Next**.

11. Lasciare immutato l'elenco dell'ordine dei campi di esportazione e fare clic su **Finish**.

VEDERE ANCHE:

Mappatura predefinita dei campi per ACT!

Creazione di file di esportazione per procedure di importazione

## Esportazione da LinkedIn®

È possibile esportare i dati dei contatti da LinkedIn in un formato di testo delimitato che successivamente si può importare.

- Aprire `www.linkedin.com/addressBookExport` e seguire la procedura presentata nella pagina utilizzando l'opzione **Microsoft Outlook (file .CSV)**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

## Esportazione da Outlook

Microsoft® Outlook® consente di esportare dati in un formato CSV (valori separati da virgola) che può successivamente essere importato.

1. Avviare Outlook.
2. Selezionare **File** > **Importa ed esporta...**.
3. Selezionare **Esporta in un file** e fare clic su **Avanti**.
4. Selezionare **Valori separati da virgola (Windows)** e fare clic su **Avanti**.

   Nota: se le virgole non sono appropriate per le proprie impostazioni internazionali, utilizzare la tabulazione o un altro delimitatore.

5. Selezionare la cartella **Referenti** e fare clic su **Avanti**. È possibile selezionare una cartella di referenti diversa se i referenti sono archiviati in più cartelle.
6. Scegliere un nome file per i dati esportati, quindi fare clic su **Avanti**
7. Fare clic su **Fine**.

VEDERE ANCHE:

Mappatura predefinita dei campi per Outlook

Creazione di file di esportazione per procedure di importazione

## Esportazione da GoldMine 4.0

GoldMine 4.0 consente di esportare dati di contatti in un formato di testo che può essere importato. Inoltre è possibile esportare le note di GoldMine 4.0 per importarle nelle organizzazioni che utilizzano le versioni Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition e Developer Edition.

- Esportazione di contatti da GoldMine 4.0
- Esportazione di note da GoldMine 4.0

### Esportazione di contatti da GoldMine 4.0

Per esportare i dati dei contatti da GoldMine 4.0, eseguire le seguenti operazioni:

1. Avviare GoldMine 4.0.
2. Scegliere **Esporta record** dal menu **Strumenti**.
3. Selezionare **Esporta in nuovo file** e **File DBF**, quindi fare clic su **Succ**.
4. Nell'elenco dei campi di GoldMine nella parte sinistra della finestra di dialogo, selezionare tutti i campi e fare clic su **Aggiungi campo**. Fare clic su **Succ**.
5. Scegliere un percorso per il file di esportazione e fare clic su **Succ**.
6. Quando viene richiesto di salvare le impostazioni, selezionare **No** e fare clic su **Succ**.
7. Fare clic su **Fine**.
8. Al termine dell'esportazione, individuare il file esportato e cambiarne l'estensione da .dbf a .csv. A questo punto il file è pronto per essere importato in Salesforce.

## Esportazione di note da GoldMine 4.0

Prima di importare le note di GoldMine 4.0 in Salesforce, è necessario importarne i contatti.

Per esportare le note da GoldMine 4.0, eseguire le seguenti operazioni:

1. Avviare GoldMine 4.0.
2. Scegliere **Esporta record** dal menu **Strumenti**.
3. Selezionare **Esporta in nuovo file** e **File ASCII**, quindi fare clic su **Succ**.
4. Nell'elenco dei campi di GoldMine nella parte sinistra della finestra di dialogo, selezionare i campi `società`, `cognome` e `note`, quindi fare clic su **Aggiungi campo**. Fare clic su **Succ**.
5. Scegliere un percorso per il file di esportazione e fare clic su **Succ**.
6. Quando viene richiesto di salvare le impostazioni, selezionare **No** e fare clic su **Succ**.
7. Fare clic su **Fine**.
8. Al termine dell'esportazione, individuare il file esportato e cambiarne l'estensione a .csv.
9. Aprire il file.
10. Aggiungere una colonna di intestazione facendo clic con il pulsante destro del mouse sulla prima riga e scegliendo **Inserisci**.
11. Nella colonna A, inserire `Società`.
12. Nella colonna B, inserire `Cognome`.
13. Nella colonna C, inserire `Nota`.
14. Se necessario, eseguire la pulitura del file prima di importarlo. È comune che siano presenti note interrotte tra le colonne, problema che si verifica quando le note contengono virgolette.

VEDERE ANCHE:

Mappatura dei campi per altre fonti di dati e importazione dell'organizzazione

Creazione di file di esportazione per procedure di importazione

# Esportazione da GoldMine 5.0

GoldMine 5.0 consente di esportare dati di contatti in un formato di testo che può essere importato. Inoltre è possibile esportare le note di GoldMine 5.0 per importarle nelle organizzazioni che utilizzano le versioni Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition e Developer Edition.

## Esportazione di contatti da GoldMine 5.0

Per esportare i dati dei contatti da GoldMine 5.0, eseguire le seguenti operazioni:

1. Avviare GoldMine 5.0.
2. Scegliere **Strumenti** > **Importazione/Esportazione guidata** > **Esporta record contatti**.
3. Selezionare **Esporta in nuovo file** e **File ASCII**, quindi fare clic su **Succ**.
4. Selezionare **Tutti i record contatti modificati** dall'elenco a discesa e fare clic su **Succ**.
5. Nell'elenco dei campi di GoldMine nella parte sinistra della finestra di dialogo, selezionare i campi che si desidera esportare e fare clic su **Aggiungi campo**. È consigliabile selezionare tutti i campi, eccetto il campo `note`. Per informazioni su come esportare le note, vedere Esportazione di note da GoldMine 5.0 a pagina 354.
6. Fare clic su **Avanti**.
7. Scegliere un percorso per il file di esportazione e selezionare la casella di controllo **Esporta nomi di campi GoldMine...**, quindi fare clic su **Succ**.
8. Quando viene richiesto di salvare le impostazioni, selezionare **No** e fare clic su **Succ**.
9. Fare clic su **Fine**.
10. Al termine dell'esportazione, individuare il file esportato e cambiarne l'estensione da .txt a .csv. A questo punto il file è pronto per essere importato in Salesforce.

## Esportazione di note da GoldMine 5.0

Prima di importare le note di GoldMine 5.0 in Salesforce, è necessario importarne i referenti.

Per esportare le note da GoldMine 5.0, eseguire le seguenti operazioni:

1. Avviare GoldMine 5.0.
2. Scegliere **Strumenti** > **Importazione/Esportazione guidata** > **Esporta record contatti**.
3. Selezionare **Esporta in nuovo file** e **File ASCII**, quindi fare clic su **Succ**.
4. Selezionare **Tutti i record contatti modificati** dall'elenco a discesa e fare clic su **Succ**.
5. Nell'elenco dei campi di GoldMine nella parte sinistra della finestra di dialogo, selezionare i campi `società`, `cognome` e `note`, quindi fare clic su **Aggiungi campo**. Fare clic su **Avanti**.
6. Scegliere un percorso per il file di esportazione e selezionare la casella di controllo **Esporta nomi di campi GoldMine...**, quindi fare clic su **Succ**.
7. Quando viene richiesto di salvare le impostazioni, selezionare **No** e fare clic su **Succ**.
8. Fare clic su **Fine**.
9. Al termine dell'esportazione, individuare il file esportato e cambiarne l'estensione da .txt a .csv.
10. Aprire il file.

11. Se necessario, eseguire la pulitura del file prima di importarlo. È comune che siano presenti note interrotte tra le colonne, problema che si verifica quando le note contengono virgolette.

VEDERE ANCHE:

Mappatura dei campi per altre fonti di dati e importazione dell'organizzazione

Creazione di file di esportazione per procedure di importazione

## Esportazione da Palm Desktop

Palm Desktop consente di esportare i referenti della Rubrica in un formato CSV (valori separati da virgola) che può successivamente essere importato.

1. Aprire la Rubrica in Palm Desktop. Se si desidera esportare solo determinati referenti, selezionare quei record.
2. Scegliere **Esporta** dal menu **File**.
3. Nella finestra di dialogo Esporta nel file, immettere il nome del file e scegliere una cartella in cui archiviarlo. Nell'elenco a discesa **Esporta come**, scegliere "Separato da virgola (*.csv;*.txt)". Selezionare l'intervallo di record da esportare: **Tutti** o **Record selezionati**.

   Nota: se le virgole non sono appropriate per le proprie impostazioni internazionali, utilizzare la tabulazione o un altro delimitatore.

4. Fare clic su **Esporta**.
5. Nella finestra di dialogo Specifica campi di esportazione, selezionare i campi della rubrica che si desidera esportare e fare clic su **OK**.

VEDERE ANCHE:

Mappatura dei campi per altre fonti di dati e importazione dell'organizzazione

Creazione di file di esportazione per procedure di importazione

## Esportazione da altre fonti di dati

È possibile importare nel sistema i dati provenienti da qualsiasi altra applicazione in grado di creare un file CSV (valori separati da virgola).

1. Salvare la fonte di dati come file CSV.

   Nota: se le virgole non sono appropriate per le proprie impostazioni internazionali, utilizzare la tabulazione o un altro delimitatore.

2. Verificare che il file contenga un solo nome per ogni campo in quanto il sistema non accetta più di un nome per campo.
3. Verificare che nel file i nomi e i titoli si trovino in due campi distinti, in quanto il sistema non accetta i campi che contengono nomi e titoli.
4. Verificare che il file contenga un solo numero di telefono per ogni campo.

VEDERE ANCHE:

Mappatura dei campi per altre fonti di dati e importazione dell'organizzazione

Creazione di file di esportazione per procedure di importazione

## Esportazione da Salesforce

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

È possibile esportare rapporti relativi ad account, referenti, oggetti personalizzati, lead o soluzioni da Salesforce per creare un file di importazione per le importazioni guidate. È necessario includere il valore `ID account`, `ID referente`, `ID oggetto personalizzato`, `ID lead` o `ID soluzione` per ogni record corrispondente nel rapporto. Tali campi ID sono identificatori univoci di Salesforce e sono utilizzati per far corrispondere correttamente i dati ai record esistenti di Salesforce.

Per creare un file di importazione con questi campi ID, è necessario innanzitutto esportare i dati da Salesforce.

1. Eseguire un rapporto relativo ad account, referenti, oggetti personalizzati, lead o soluzioni in Salesforce, includere il rispettivo campo ID, quindi esportarlo in Excel.
2. Se si esportano sia lead che referenti a cui sarà destinata una campagna:
   a. Combinare i rapporti esportati in un solo file CSV in Excel. Assicurarsi che i valori del campo ID si trovino nella stessa colonna.

      Nota: se le virgole non sono appropriate per le proprie impostazioni internazionali, utilizzare la tabulazione o un altro delimitatore.

   b. Rinominare la colonna `ID lead/ID referente` in `ID record`.
   c. Aggiungere la colonna `Stato` e inserire lo stato membro della campagna per ciascun referente o lead.

VEDERE ANCHE:

Creazione di file di esportazione per procedure di importazione

# Preparazione dei dati per l'importazione

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

Dopo avere esportato i dati da Salesforce o dall'applicazione esistente, prepararli per l'importazione.

Nota: se i dati presentano informazioni in campi che non corrispondono ad alcuno dei campi standard, l'amministratore può creare campi personalizzati per tali dati prima dell'importazione.

I campi universalmente obbligatori devono essere inclusi nei file di importazione; in caso contrario, l'importazione non andrà a buon fine.

**Preparazione dei referenti**

Quando si importa da ACT! o da Outlook, la procedura guidata Importa referenti personali mappa automaticamente i campi da ACT! e Outlook a Salesforce.

Quando si importa da altre fonti di dati è necessario utilizzare Excel® per etichettare le colonne nel file di importazione come specificato in Mappatura dei campi per altre fonti di dati e importazione dell'organizzazione a pagina 363.

**Preparazione degli Account personali.**

Quando si importano gli account personali, utilizzare le etichette dei campi di Salesforce come etichette delle colonne del file di importazione.

**Preparazione degli account aziendali e dei referenti dell'organizzazione**

Per l'importazione di account aziendali e referenti dell'organizzazione è necessario utilizzare Excel® per assegnare etichette alle colonne del file di importazione come specificato in Mappatura dei campi per altre fonti di dati e importazione dell'organizzazione a pagina 363.

**Preparazione dei lead dell'organizzazione**

Quando si importano lead generali o lead per le campagne, utilizzare le etichette del file di importazione specificate in Mappatura dei campi per l'importazione di lead a pagina 368.

**Preparazione degli oggetti personalizzati**

Quando si importa un oggetto personalizzato, utilizzare le etichette di campo mostrate nella pagina dei dettagli dell'oggetto personalizzato in Salesforce come etichette di colonne nel file di importazione.

**Preparazione delle soluzioni**

Quando si importano soluzioni, utilizzare le etichette di campo in Salesforce come etichette di colonne nel file di importazione.

È possibile inserire codice HTML nelle soluzioni che si prevede di importare in Salesforce. Tuttavia, a meno che l'organizzazione non abbia abilitato le soluzioni HTML, i tag HTML verranno visualizzati nelle soluzioni dopo l'importazione.

Ai fini della sicurezza, Salesforce filtra automaticamente tutte le soluzioni HTML per verificare la presenza di codice HTML potenzialmente dannoso. Se viene rilevato un codice HTML potenzialmente dannoso in una soluzione HTML, Salesforce procede a eliminarlo automaticamente o a trasformarlo in formato testo per gli utenti che visualizzano la soluzione HTML. Tenere presente che gli utenti non saranno in grado di notare quando codice HTML potenzialmente dannoso viene rimosso da una soluzione HTML.

È possibile importare in Salesforce soluzioni scritte in formato HTML. Tuttavia, per ragioni di sicurezza, sono consentiti solo i tag HTML elencati di seguito. Il contenuto dei tag HTML non presenti in elenco viene automaticamente rimosso quando viene salvato all'interno di soluzioni HTML. Inoltre, il contenuto di tutti i tag `<script>` e `<iframe>`, nonché tutto il codice JavaScript, vengono automaticamente rimossi quando vengono salvati nelle soluzioni HTML. Infine, i fogli di stile CSS non sono supportati nelle soluzioni HTML.

Nelle soluzioni HTML importate in Salesforce sono consentiti i seguenti tag HTML:

| <a> | <dt> | <q> |
|---|---|---|
| <abbr> | <em> | <samp> |
| <acronym> | <font> | <small> |
| <address> | <h1> | <span> |
| <b> | <h2> | <strike> |
| <bdo> | <h3> | <strong> |
| <big> | <h4> | <sub> |
| <blockquote> | <h5> | <sup> |
| <br> | <h6> | <table> |
| <caption> | <hr> | <tbody> |
| <cite> | <i> | <td> |
| <code> | <img> | <tfoot> |
| <col> | <ins> | <th> |
| <colgroup> | <kbd> | <thead> |
| <dd> | <li> | <tr> |
| <del> | <ol> | <tt> |

| | | |
|---|---|---|
| `<dfn>` | `<p>` | `<ul>` |
| `<div>` | `<pre>` | `<var>` |
| `<dl>` | | |

All'interno dei tag riportati sopra, è possibile includere i seguenti attributi:

| | | |
|---|---|---|
| alt | face | size |
| background | height | src |
| border | href | style |
| class | name | target |
| colspan | rowspan | width |

Gli attributi riportati sopra possono includere un URL ma sono limitati a URL che iniziano con:

- http:
- https:
- file:
- ftp:
- mailto:
- #
- / per i rispettivi link

VEDERE ANCHE:

Mappatura predefinita dei campi per ACT!

Mappatura predefinita dei campi per Outlook

Creazione di file di esportazione per procedure di importazione

## Mappatura predefinita dei campi per ACT!

Questa tabella mostra nei dettagli la mappatura dei campi di ACT! nei campi di importazione account e referente di Salesforce durante un'importazione di dati singola.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

Nota: se un record ACT! contiene più referenti per la stessa società, l'importazione guidata crea più referenti per tale account.

| ACT! Campo | Campo di importazione |
|---|---|
| Indirizzo 1 | Referente: Indirizzo postale e<br>Account: Indirizzo di fatturazione |

| ACT! Campo | Campo di importazione |
|---|---|
| Indirizzo 2 | Referente: Indirizzo postale e<br>Account: Indirizzo di fatturazione |
| Indirizzo 3 | Referente: Indirizzo postale e<br>Account: Indirizzo di fatturazione |
| Telefono alt. | Referente: Altro telefono |
| Int. telefono alt. | Referente: Altro interno |
| Assistente | Referente: Nome assistente |
| Telefono assist. | Referente: Telefono assist. |
| Interno assist. | Referente: Interno assist. |
| Città | Referente: Città indirizzo postale e<br>Account: Città fatturazione |
| Società | Account: Nome |
| Referente | Referente: Nome completo |
| Paese | Referente: Paese indirizzo postale e<br>Account: Paese fatturazione |
| Reparto | Referente: Reparto |
| Accesso email<br>(la procedura guidata di importazione verifica la validità dell'indirizzo email secondo il formato mrossi@acme.com) | Referente: Email |
| Fax | Referente: Fax e<br>Account: Fax |
| Int. fax. | Referente: Interno fax (uff.) |
| Nome | Referente: Nome |
| Indirizzo 1 (abit.) | Referente: Altro indirizzo 1 |
| Indirizzo 2 (abit.) | Referente: Altro indirizzo 2 |
| Indirizzo 3 (abit.) | Referente: Altro indirizzo 3 |
| Città (abit.) | Referente: Altra città |
| Paese (abit.) | Referente: Altro paese |
| Telefono abitazione | Referente: Telefono abitazione |
| Provincia (abit.) | Referente: Altra provincia |

| ACT! Campo | Campo di importazione |
|---|---|
| CAP abitazione | Referente: Altro CAP |
| ID/Stato | Account: Tipo |
| Cognome | Referente: Cognome |
| Telefono cellulare | Referente: Telefono cellulare |
| Nota | Non viene importato |
| Telefono | Referente: Telefono e<br>Account: Telefono |
| Int. telefono | Referente: Interno (uff.) |
| Segnalato da | Referente: Fonte del lead |
| Reddito | Account: Reddito annuale |
| Provincia | Referente: Provincia indirizzo postale e<br>Account: Provincia fatturazione |
| Simbolo ticker | Account: Simbolo ticker |
| Qualifica | Referente: Qualifica |
| Sito Web | Account: Sito Web |
| CAP | Referente: CAP indirizzo postale<br>Account: CAP fatturazione |
| Secondo referente | Secondo referente: Nome |
| Secondo telefono | Secondo referente: Telefono |
| Secondo Int. telefono | Secondo referente: Int. telefono |
| Seconda qualifica | Secondo referente: Qualifica |
| Terzo referente | Terzo referente: Nome |
| Terzo telefono | Terzo referente: Telefono |
| Terzo int. telefono | Terzo referente: Int. telefono |
| Terza qualifica | Terzo referente: Qualifica |
| 2o ultimo contatto, 3o ultimo contatto, Titolo assist., Ultimo tentativo, Ultima riunione, Ultimo contatto, Ultimi risultati, Data lettera, Cercapersone, Coniuge, Utente 1-15 | Referente: Nota o account: Nota<br>Nelle organizzazioni che utilizzano le versioni Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition e Developer Edition si specifica quali campi importare in una sola |

| ACT! Campo | Campo di importazione |
|---|---|
| | nota referente o nota account; non vengono create note separate per ciascun campo di ACT!. |

VEDERE ANCHE:

- Esportazione da ACT!
- Preparazione dei dati per l'importazione

## Mappatura predefinita dei campi per Outlook

Questa tabella mostra nei dettagli la mappatura dei campi di Outlook nei campi di importazione account e referente di Salesforce durante un'importazione di dati singola.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

| Campo di Outlook | Campo di importazione |
|---|---|
| `Nome assistente` | Referente: `Nome assistente` |
| `Telefono assistente` | Referente: `Telefono assist.` |
| `Data di nascita` | Referente: `Compleanno` |
| `Città (uff.)` | Referente: `Città indirizzo postale` e<br>Account: `Città fatturazione` |
| `Paese (uff.)` | Referente: `Paese indirizzo postale` e<br>Account: `Paese fatturazione` |
| `Fax (uff.)` | Referente: `Fax` e<br>Account: `Fax` |
| `Telefono (uff.)` | Referente: `Telefono` |
| `CAP (uff.)` | Referente: `CAP indirizzo postale`<br>Account: `CAP fatturazione` |
| `Via (uff.)` | Referente: `Indirizzo postale` e<br>Account: `Indirizzo di fatturazione` |
| `Via (uff.) 2` | Referente: `Indirizzo postale` e<br>Account: `Indirizzo di fatturazione` |

| Campo di Outlook | Campo di importazione |
|---|---|
| Via (uff.) 3 | Referente: Indirizzo postale e<br>Account: Indirizzo di fatturazione |
| Società | Account: Nome account e<br>Referente: Account |
| Telefono principale società | Account: Telefono |
| Reparto | Referente: Reparto |
| Email<br>(la procedura guidata di importazione verifica la validità dell'indirizzo email secondo il formato mrossi@acme.com) | Referente: Email |
| Nome | Referente: Nome |
| Città (abit.) | Referente: Altra città |
| Paese (abit.) | Referente: Altro paese |
| Telefono abitazione | Referente: Telefono abitazione |
| CAP (ab.) | Referente: Altro CAP |
| Via (ab.) | Referente: Altro indirizzo |
| Via (ab.) 2 | Referente: Altro indirizzo |
| Via (ab.) 3 | Referente: Altro indirizzo |
| Qualifica | Referente: Qualifica |
| Cognome | Referente: Cognome |
| Nome manager | Referente: Fa capo a<br>(se il nome in questo campo non corrisponde a un referente esistente, viene creato un nuovo referente con il nome del manager) |
| Telefono cellulare | Referente: Telefono cellulare |
| Note | Referente: Descrizione |
| Altro telefono | Referente: Altro telefono |
| Segnalato da | Referente: Fonte del lead |
| Qualifica | Referente: Titolo |
| Pagina Web | Account: Sito Web |

| Campo di Outlook | Campo di importazione |
| --- | --- |
| `Account`, `Anniversario`, `Dati fatturazione`, `Telefono (uff.) 2`, `Richiamata automatica`, `Telefono auto`, `Categorie`, `Figli`, `Server di elenchi in linea`, `Email 2`, `Email 3`, `Cod. Fisc./P. IVA`, `Hobby`, `Fax (ab.)`, `Telefono (ab.) 2`, `Indirizzo disponibilità Internet`, `ISDN`, `Parole chiave`, `Lingua`, `Luogo`, `Secondo nome`, `Indennità trasferta`, `Ubicazione ufficio`, `Numero ID organizzativo`, `Altra città`, `Altro paese`, `Altro fax`, `Altro codice postale`, `Altra provincia`, `Altra via`, `Altra via 2`, `Altra via 3`, `Cercapersone`, `Casella postale`, `Telefono principale`, `Professione`, `Radiotelefono`, `Coniuge`, `Suffisso`, `Telex`, `Telefono TTY/TDD`, `Utente 1`, `Utente 2`, `Utente 3`, `Utente 4` | Referente: `Nota` o account: `Nota`<br>Nelle organizzazioni che utilizzano le versioni Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition e Developer Edition si specifica quali campi importare in una sola nota referente o nota account; non vengono create note separate per ciascun campo di Outlook. |

VEDERE ANCHE:

Esportazione da Outlook

Preparazione dei dati per l'importazione

## Mappatura dei campi per altre fonti di dati e importazione dell'organizzazione

In caso di importazione di account e di referenti per un'organizzazione o di importazione di singoli dati da fonti diverse da Outlook o ACT!, le importazioni guidate mappano i campi con la maggiore correttezza possibile. È necessario regolare la mappatura prima che l'importazione sia terminata. Prima di importare i dati, Salesforce consiglia di utilizzare Excel per assegnare alle colonne nel file di importazione le etichette elencate di seguito.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

Importazione organizzazione non disponibile nella versione: **Personal Edition**, **Database.com Edition**

> Nota: Le mappature predefinite elencate di seguito costituiscono una guida per l'importazione, non assicurano l'accuratezza al 100% nella mappatura dei dati. **È necessario regolare la mappatura tramite le importazioni guidate.** Si ricorda che è possibile mappare più volte lo stesso campo se necessario, ad esempio per i campi dell'indirizzo del referente e dell'account.

**Campi comuni per referenti e account**

| Etichetta per il file di importazione | Campo Salesforce |
| --- | --- |
| `Titolare record`<br>Nota: Per le importazioni singole questo campo non è necessario poiché si è automaticamente titolare di tutti i dati importati. Inoltre, quando si importano record per ID record di Salesforce, il campo viene ignorato.) | Referente: `Titolare referente` e<br>Account: `Titolare account` |

**Campi comuni per referenti e account**

| Etichetta per il file di importazione | Campo Salesforce |
| --- | --- |
| `Codice ISO valuta`<br>Nota: è possibile utilizzare questo campo solo per le importazioni in organizzazioni che utilizzano più valute. Per ulteriori informazioni, vedere Importazione di più valute a pagina 349. | Referente: `Valuta referente` e<br>Account: `Valuta account` |

**Campi referente**

| Etichetta per il file di importazione | Campo Salesforce |
| --- | --- |
| `Assistente` | Referente: `Assistente` |
| `Telefono assist.` | Referente: `Telefono assist.` |
| `Interno assist.` | Aggiunto al referente: `Telefono assist.` |
| `Data di nascita` | Referente: `Data di nascita` |
| `Fax (uff.)` | Referente: `Fax` |
| `Interno fax (uff.)` | Aggiunto al referente: `Fax` |
| `Telefono (uff.)` | Referente: `Telefono` |
| `Interno (uff.)` | Aggiunto al referente: `Telefono` |
| `Descrizione referente` | Referente: `Descrizione` |
| `Nome completo referente` *oppure*<br>`Nome` e `Cognome`<br>Nota: quando si importano i nomi dei referenti, utilizzare `Nome completo referente` o `Nome` e `Cognome`, ma non entrambi.) | Referente: `Nome` e<br>Referente: `Cognome` |
| `ID referente`<br>Nota: gli ID record fanno distinzione tra maiuscole e minuscole e non possono essere modificati. | Referente: `ID referente` |
| `Nota referente` | Crea una nota allegata al referente |
| `Reparto` | Referente: `Reparto` |
| `Indirizzo email`<br>(Nota: la procedura guidata di importazione verifica la validità dell'indirizzo di posta elettronica secondo il formato: mrossi@acme.com) | Referente: `Email` |
| `Fuori lista email` | Referente: `Fuori lista email` |

**Campi referente**

| Etichetta per il file di importazione | Campo Salesforce |
| --- | --- |
| (Nota: utilizzare "1" per indicare che l'utente è fuori lista posta elettronica; utilizzare "0" per indicare che l'utente desidera messaggi di posta elettronica.) | |
| Telefono abitazione | Referente: Telefono abitazione |
| Interno telefono (abit.) | Aggiunto al referente: Telefono abitazione |
| Fonte del lead | Referente: Fonte del lead |
| Città indirizzo postale | Referente: Città indirizzo postale |
| Paese indirizzo postale | Referente: Paese indirizzo postale |
| CAP indirizzo postale | Referente: CAP indirizzo postale |
| Provincia indirizzo postale | Referente: Stato/Provincia indirizzo postale |
| Via indirizzo postale 1 | Referente: Indirizzo postale |
| Via indirizzo postale 2 | Referente: Indirizzo postale |
| Via indirizzo postale 3 | Referente: Indirizzo postale |
| Telefono cellulare | Referente: Cellulare |
| Int. cellulare | Aggiunto al referente: Cellulare |
| Altra città | Referente: Altra città |
| Altro paese | Referente: Altro paese |
| Altro telefono | Referente: Altro telefono |
| Altro interno | Aggiunto al referente: Altro telefono |
| Altro CAP | Referente: Altro CAP |
| Altra provincia | Referente: Altro stato/provincia |
| Altra via 1 | Referente: Altro indirizzo |
| Altra via 2 | Referente: Altro indirizzo |
| Altra via 3 | Referente: Altro indirizzo |
| Fa capo a<br>(Nota: se con l'importazione guidata non è possibile trovare un referente corrispondente al nome contenuto in questo campo, viene creato un nuovo referente utilizzando questo valore come referente Nome e Cognome.) | Referente: Fa capo a |
| Titolo | Anteposto al referente: Nome |
| Qualifica | Referente: Qualifica |

**Campi referente**

| Etichetta per il file di importazione | Campo Salesforce |
|---|---|
| `Secondo referente` | Dividi in referenti: `Nome` e `Cognome` per un secondo referente per l'account |
| `Secondo telefono` | Referente: `Telefono` per un secondo referente per l'account |
| `Secondo Int. telefono` | Aggiunto al referente: `Telefono` per un secondo referente per l'account |
| `Seconda qualifica` | Referente: `Qualifica` per un secondo referente per l'account |
| `Terzo referente` | Dividi in referenti: `Nome` e `Cognome` per un terzo referente per l'account |
| `Terzo telefono` | Referente: `Telefono` per un terzo referente per l'account |
| `Terzo int. telefono` | Aggiunto al referente: `Telefono` per un terzo referente per l'account |
| `Terza qualifica` | Referente: `Qualifica` per un terzo referente per l'account |

**Campi account**

| Etichetta per il file di importazione | Campo Salesforce |
|---|---|
| `Descrizione account` | Account: `Descrizione` |
| `Divisione account`<br>(Nota: non è necessario specificare questo campo se si sceglie di assegnare la divisione tramite l'elenco a discesa nella fase 1 dell'Importazione guidata. Se non si mappa questo campo o non si utilizza l'elenco a discesa delle divisioni, per ogni record la divisione viene impostata sulla divisione predefinita del titolare del record.) | Account: `Divisione account` |
| `Fax account` | Account: `Fax` |
| `Interno fax account` | Aggiunto all'account: `Fax` |
| `ID account`<br>Nota: gli ID record fanno distinzione tra maiuscole e minuscole e non possono essere modificati. | Account: `ID account` |
| `Nome account` | Account: `Nome account` e<br>Referente: `Account` |
| `Nota account` | Crea una nota allegata all'account |
| `Numero account` | Account: `Numero account` |
| `Telefono account` | Account: `Telefono` |

**Campi account**

| Etichetta per il file di importazione | Campo Salesforce |
| --- | --- |
| Interno account | Aggiunto all'account: Telefono |
| Sito account | Account: Sito account |
| Tipo account | Account: Tipo |
| Città fatturazione | Account: Città fatturazione |
| Paese fatturazione | Account: Paese fatturazione |
| CAP fatturazione | Account: CAP fatturazione |
| Provincia fatturazione | Account: Stato/Provincia fatturazione |
| Via fatturazione 1 | Account: Indirizzo di fatturazione |
| Via fatturazione 2 | Account: Indirizzo di fatturazione |
| Via fatturazione 3 | Account: Indirizzo di fatturazione |
| Dipendenti | Account: Dipendenti |
| Settore | Account: Settore |
| Proprietà | Account: Proprietà |
| Società controllante<br>Nota: se con l'importazione guidata non è possibile trovare un account corrispondente al nome società controllante, viene creato un nuovo account utilizzando questo valore come Nome account.) | Account: Società controllante |
| Sito società controllante<br>(Nota: indica il valore del sito per la Società controllante.) | Account: Sito account<br>(Nota: mappa nel campo Sito account nella società controllante.) |
| Valutazione | Account: Valutazione |
| Reddito | Account: Reddito annuale |
| Città spedizione | Account: Città spedizione |
| Paese spedizioni | Account: Paese spedizioni |
| CAP spedizione | Account: CAP spedizioni |
| Provincia spedizioni | Account: Stato/Provincia spedizioni |
| Via spedizione 1 | Account: Indirizzo spedizione |
| Via spedizione 2 | Account: Indirizzo spedizione |
| Via spedizione 3 | Account: Indirizzo spedizione |

**Campi account**

| Etichetta per il file di importazione | Campo Salesforce |
| --- | --- |
| Codice SIC | Account: Codice SIC |
| Simbolo ticker | Account: Simbolo ticker |
| Sito Web | Account: Sito Web |

VEDERE ANCHE:

Preparazione dei dati per l'importazione

## Mappatura dei campi per l'importazione di lead

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Quando si importano i lead, le procedure Importazione guidata dati e Importa lead delle campagne mappano i campi nel file di importazione nel modo più corretto possibile, ma è necessario regolare la mappatura prima di completare l'importazione. Prima di importare i lead, è consigliabile utilizzare Excel per assegnare alle colonne nel file di importazione le etichette elencate nella tabella che segue.

Nota: Le seguenti mappature predefinite vengono offerte come guida. Non garantiscono una precisione al 100% della mappatura dei dati, quindi sarà necessario perfezionare la mappatura nella procedura di importazione guidata.

| Etichetta per il file di importazione | Campo lead di Salesforce |
| --- | --- |
| Reddito annuale | Reddito annuale |
| Città | Città |
| Società | Società |
| Paese | Paese |
| Codice ISO valuta<br>(Nota: è possibile utilizzare questo campo solo per le organizzazioni che utilizzano più valute; vedere Importazione di più valute a pagina 349.) | Valuta lead |
| Descrizione | Descrizione |
| Email<br>(la procedura guidata di importazione verifica la validità dell'indirizzo email secondo il formato mrossi@acme.com) | Email |
| Fuori lista email | Fuori lista email |

| Etichetta per il file di importazione | Campo lead di Salesforce |
| --- | --- |
| (Utilizzare “1” per indicare che l'utente è fuori lista email; utilizzare “0” per indicare che l'utente desidera messaggi email). | |
| N. di dipendenti | N. di dipendenti |
| Fax | Fax |
| Name completo oppure Nome e Cognome<br>(Nota: quando si importano i nomi dei lead, utilizzare Nome completo o Nome e Cognome, ma non entrambi.) | Nome e Cognome |
| Settore | Settore |
| Divisione lead<br>(Nota: non è necessario specificare questo campo se si sceglie di assegnare la divisione tramite l'elenco a discesa nella fase 1 dell'Importazione guidata. Se non si mappa questo campo o non si utilizza l'elenco a discesa delle divisioni, per ogni record la divisione viene impostata sulla divisione predefinita del titolare del record.) | Divisione lead |
| ID lead<br>(Nota: gli ID record fanno distinzione tra maiuscole e minuscole e non possono essere modificati. | ID lead |
| Fonte del lead<br>Nota: Non è necessario specificare questo campo se si sceglie di assegnare lo stesso Fonte del lead a tutti i lead nella prima pagina dell'importazione guidata. | Fonte del lead |
| Stato lead | Stato lead |
| Telefono cellulare | Cellulare |
| Telefono | Telefono |
| CAP | CAP |
| Valutazione | Valutazione |
| Titolare record<br>Nota: questo campo non è necessario se si assegna la proprietà tramite una regola di assegnazione del lead. Inoltre, quando si importano record per ID record di Salesforce, il campo viene ignorato.) | Titolare lead |
| Titolo | Aggiunto all'inizio del Nome |

| Etichetta per il file di importazione | Campo lead di Salesforce |
|---|---|
| Provincia | Stato |
| Stato<br>(solo per l'Importazione guidata delle campagne.) | Stato<br>(nell'elenco correlato Cronologia campagne di un lead) |
| Via 1 | Indirizzo |
| Via 2 | Indirizzo |
| Via 3 | Indirizzo |
| Qualifica | Qualifica |
| Sito Web | Sito Web |

Se si includono tipi di record in questo elenco, la procedura Importazione guidata dati utilizza il tipo di record predefinito del titolare record durante la creazione di nuovi record. Per i record esistenti, l'Importazione guidata dati non aggiorna il campo Tipo di record.

Se si sceglie di utilizzare regole di assegnazione, la procedura Importazione guidata dati utilizza il tipo di record predefinito del nuovo titolare durante la creazione di nuovi record. Quando le regole di assegnazione assegnano il record a un'area di attesa, viene utilizzato il tipo di record predefinito del titolare dell'area di attesa.

VEDERE ANCHE:

Preparazione dei dati per l'importazione

# Importazione di referenti personali da Outlook o ACT!

I singoli utenti possono importare fino a 500 referenti e account aziendali da Outlook o ACT! con la procedura guidata Importa referenti personali.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne Database.com Edition

AUTORIZZAZIONI UTENTE

Per importare i referenti e gli account personali:
- "Importa referenti personali"

Importante: Salesforce ha sostituito le singole procedure di importazione guidata per account, referenti e altri oggetti con una procedura unificata di Importazione guidata dati (le singole procedure di importazione guidata si aprono in piccole finestre popup, mentre l'importazione unificata si apre in un browser di dimensioni normali con dataimporter.app alla fine dell'URL). Per iniziare a utilizzare la procedura unificata, da Imposta, immettere *Importazione guidata dati* nella casella Ricerca veloce, quindi selezionare **Importazione guidata dati**. (le opzioni visualizzate dipendono dalle autorizzazioni di cui si dispone).

Prima di avviare la procedura guidata Importa referenti personali, creare un file di esportazione e preparare correttamente i dati. Se non si sta effettuando l'importazione da ACT! o da Outlook, vedere le istruzioni in Importazione referenti personali da altre fonti.

Suggerimento: I dati possono essere importati solo nei campi che è possibile modificare.

1. Dalle impostazioni personali, immettere *Importa* nella casella Ricerca veloce, selezionare **Importa account e referenti dell'organizzazione** e fare clic su **Avviare l'importazione guidata**. In alternativa, fare clic sul link **Importa account e referenti dell'organizzazione** nell'area degli strumenti della pagina iniziale Account.

Le etichette dei referenti e degli account aziendali potrebbero essere state rinominate dall'amministratore; in questo caso i link relativi all'importazione potrebbero contenere testo personalizzato.

2. Specificare se la fonte dei dati è ACT! o Outlook. Fare clic su **Avanti**.
3. Fare clic su **Scegli file** per caricare il file.

   Nota: Importare un piccolo file di prova per accertarsi che il file di importazione sia stato preparato correttamente.

4. Se lo si desidera, fare clic su **Personalizza mappature** per verificare le mappature dei campi.
5. Fare clic su **Importa ora** per completare l'importazione.

IN QUESTA SEZIONE:

Importazione referenti personali da altre fonti

Con la procedura guidata Importa referenti personali, è possibile importare un massimo di 500 referenti e account aziendali associati praticament da qualsiasi fonte.

Importazione degli account personali

Importa account personali dell'organizzazione

Importazione guidata dati

Importazione guidata dati offre un'interfaccia unificata che consente di importare dati per numerosi oggetti Salesforce standard, inclusi account, referenti, lead e soluzioni. La procedura guidata consente anche di importare dati per gli oggetti personalizzati.

Domande frequenti su Importazione guidata dati

VEDERE ANCHE:

Importazione guidata dati

Cosa viene importato per gli oggetti personalizzati?

Creazione di file di esportazione per procedure di importazione

Esportazione da ACT!

Esportazione da Outlook

Preparazione dei dati per l'importazione

Mappatura dei campi per altre fonti di dati e importazione dell'organizzazione

Panoramica sull'importazione

# Importazione referenti personali da altre fonti

Con la procedura guidata Importa referenti personali, è possibile importare un massimo di 500 referenti e account aziendali associati praticament da qualsiasi fonte.

Prima di avviare la procedura guidata Importa referenti personali, creare un file di esportazione e preparare correttamente i dati. Se si sta effettuando l'importazione da ACT! o da Outlook, vedere Importazione referenti personali da Outlook o ACT!.

Il file di esportazione deve essere in formato delimitato da virgole (.csv).

Suggerimento: I dati possono essere importati solo nei campi che è possibile modificare.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

AUTORIZZAZIONI UTENTE

Per importare i referenti personali:

- "Lettura", "Crea", "Modifica" ed "Elimina" per i referenti

  E

  "Modifica tutti i dati" per i referenti

1. Dalle impostazioni personali, immettere *Importa* nella casella Ricerca veloce, selezionare **Importa account e referenti dell'organizzazione** e fare clic su **Avvia la procedura di importazione**. In alternativa, fare clic sul link **Importa account e referenti dell'organizzazione** nell'area degli strumenti della pagina iniziale Account.

   Le etichette dei referenti e degli account aziendali potrebbero essere state rinominate dall'amministratore; in questo caso i link relativi all'importazione potrebbero contenere testo personalizzato.

2. Fare clic su **Avanti**.
3. Fare clic su **Scegli file** per caricare il file.

   Nota: Importare un piccolo file di prova per accertarsi che il file di importazione sia stato preparato correttamente.

4. Se necessario, modificare l'impostazione predefinita di codifica dei caratteri.
5. Scegliere se i duplicati dovranno essere individuati mediante l'indirizzo email o il nome, quindi fare clic su **Avanti**.
6. Per assicurarsi che i dati dei referenti vengano immessi nei campi appropriati, rivedere le mappature predefinite e modificare quelle eventualmente inesatte, quindi fare clic su **Avanti**.
   - L'utente che esegue l'importazione viene automaticamente assegnato come titolare dei referenti o account aziendali importati; pertanto non è necessario eseguire la mappatura a un campo `Titolare record`.
   - Selezionare `Sovrascrivi valori di account esistenti` se si desidera sovrascrivere le informazioni esistenti sugli account aziendali con i dati importati. I dati esistenti non saranno eliminati se i campi dei dati importati sono vuoti.
   - I dati possono essere importati solo nei campi che è possibile modificare.

7. Se alcuni campi non vengono mappati, e l'organizzazione è una versione Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition o Developer Edition, è possibile scegliere di non importare i campi non mappati oppure di gestire i dati dei campi non mappati all'interno di una Nota per il referente o l'account aziendale. Tutti i dati importati non mappati per un record vengono inclusi in un'unica nota.

8. Fare clic su **Importa ora** per completare l'importazione.

VEDERE ANCHE:

Importazione guidata dati

Cosa viene importato per gli oggetti personalizzati?

Creazione di file di esportazione per procedure di importazione

Preparazione dei dati per l'importazione

Mappatura dei campi per altre fonti di dati e importazione dell'organizzazione

Panoramica sull'importazione

## Importazione degli account personali

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

L'importazione di account personali è disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per importare i propri account personali:

- "Crea" per gli account

  E

  "Lettura" per i referenti

  E

  "Importa referenti personali"

  E

  Almeno un tipo di record account personale disponibile nel proprio profilo o negli insiemi di autorizzazioni

Importante: Salesforce ha sostituito le singole procedure di importazione guidata per account, referenti e altri oggetti con una procedura unificata di Importazione guidata dati (le singole procedure di importazione guidata si aprono in piccole finestre popup, mentre l'importazione unificata si apre in un browser di dimensioni normali con dataimporter.app alla fine dell'URL). Per iniziare a utilizzare la procedura unificata, da Imposta, immettere *Importazione guidata dati* nella casella `Ricerca veloce`, quindi selezionare **Importazione guidata dati**. (le opzioni visualizzate dipendono dalle autorizzazioni di cui si dispone).

Con la procedura guidata Importa account personali è possibile importare gli account personali di cui si è titolari. Per capire come viene individuata la corrispondenza tra i record di account personali ed evitare la creazione di duplicati, vedere Quali elementi vengono importati per gli account personali? a pagina 343.

Nota: è possibile che l'amministratore abbia rinominato "account personale". In questo caso la procedura guidata di importazione farà riferimento al nuovo nome.

Per importare gli account personali, eseguire le operazioni descritte di seguito. Per maggiori dettagli, fare clic sui link seguenti:

1. Avviare la procedura guidata
2. xEvitare record duplicati a pagina 374
3. Selezionare i tipi di record a pagina 374
4. Caricare il file di importazione a pagina 374
5. Mappare i campi a pagina 374
6. Confermare e inviare la richiesta di importazione a pagina 374
7. Completare l'importazione a pagina 375

### Avviare la procedura guidata

1. Per importare gli account personali, dalle impostazioni personali, immettere *Importa*, quinfi selezionare **Importa account personali**.

   In alternativa, fare clic su **Importa account personali** nell'area degli strumenti della pagina iniziale Account.

2. Per ottenere risultati ottimali, eseguire tutte le operazioni indicate nella pagina introduttiva.

3. Fare clic su **Avviare l'importazione guidata** per iniziare l'importazione.

## Evitare record duplicati

1. Scegliere il campo da utilizzare per la ricerca di corrispondenze tra i record esistenti in Salesforce e i record nel file di importazione. L'opzione `ID esterno` è disabilitata se non è stato creato alcun campo di ID esterno per i record.
2. Specificare l'operazione da eseguire se vengono individuate corrispondenze: importare solo i nuovi record, aggiornare solo i record esistenti oppure aggiornare i record esistenti e importare quelli nuovi.

   Nota: Se si seleziona la ricerca di corrispondenze per `ID Salesforce`, è possibile solo aggiornare i record esistenti ma non importare quelli nuovi.

3. Fare clic su **Avanti**.

## Selezionare il tipo di record

1. Scegliere il tipo di record che si desidera assegnare ai record nel file di importazione.
2. Se si inseriscono nuovi record e si aggiornano i record esistenti contemporaneamente, specificare se si desidera ignorare i tipi di record dei record esistenti.
3. Fare clic su **Avanti**.

## Caricare il file di importazione

1. Fare clic su **Sfoglia...** per specificare il percorso del file di importazione.
2. Selezionare la codifica dei caratteri del file di importazione. Nella maggior parte dei casi è possibile accettare il valore predefinito.
3. Specificare le impostazioni aggiuntive a seconda della configurazione dell'organizzazione, ad esempio se devono essere attivate le regole di flusso di lavoro e la lingua dei record nel file di importazione.
4. Fare clic su **Avanti**.

## Mappare i campi

1. Mappare i campi nel file di importazione con i campi appropriati di Salesforce ricercando la corrispondenza tra i campi sulla sinistra, che comprendono tutte le colonne del file di importazione, e il campo appropriato di Salesforce sulla destra. Se le etichette di colonna nel file di importazione corrispondono esattamente alle etichette di campo in Salesforce, tali campi verranno mappati automaticamente. Se invece due o più etichette di colonna del file corrispondono esattamente a un campo in Salesforce, tali campi dovranno essere mappati manualmente.

   Nota: Alcuni campi di Salesforce non possono essere aggiornati utilizzando l'importazione, ad esempio `Data creazione` e `Data ultima modifica`. Quindi, anche se si utilizza un rapporto esportato come file di importazione, alcuni campi di Salesforce nel file non potranno essere mappati.

2. Fare clic su **Avanti**. Se non sono stati mappati tutti i campi nel file di importazione, verrà visualizzato un avviso. I valori dei campi non mappati non vengono importati.

## Confermare e inviare la richiesta di importazione

1. Leggere tutti i messaggi di avviso visualizzati durante l'importazione guidata. Se lo si desidera, fare clic su **Indietro** per tornare a una fase precedente e risolvere eventuali problemi.
2. Scegliere **Importa ora** per inviare la richiesta di importazione a Salesforce.

## Completare l'importazione

1. Viene visualizzato un messaggio in cui è riportata la durata approssimativa dell'importazione. Al termine dell'operazione di importazione, verrà inviato un messaggio dell'Assistenza clienti all'indirizzo email visualizzato.
2. Fare clic su **Fine** per terminare la procedura guidata.
3. Per monitorare lo stato delle importazioni in sospeso, da Imposta, fare clic su **Monitoraggio** > **Importazioni**.

VEDERE ANCHE:

Importazione guidata dati

Creazione di file di esportazione per procedure di importazione

Preparazione dei dati per l'importazione

Panoramica sull'importazione

# Importa account personali dell'organizzazione

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

L'importazione di account personali è disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per importare gli account personali dell'organizzazione:

- "Modifica tutti i dati"

Importante: Salesforce ha sostituito le singole procedure di importazione guidata per account, referenti e altri oggetti con una procedura unificata di Importazione guidata dati (le singole procedure di importazione guidata si aprono in piccole finestre popup, mentre l'importazione unificata si apre in un browser di dimensioni normali con dataimporter.app alla fine dell'URL). Per iniziare a utilizzare la procedura unificata, da Imposta, immettere *Importazione guidata dati* nella casella `Ricerca veloce`, quindi selezionare **Importazione guidata dati**. (le opzioni visualizzate dipendono dalle autorizzazioni di cui si dispone).

Con la procedura guidata Importa account personali dell'organizzazione è possibile importare gli account personali di cui sono titolari altri utenti. Per capire come viene individuata la corrispondenza tra i record di account personali ed evitare la creazione di duplicati, vedere Quali elementi vengono importati per gli account personali? a pagina 343.

Nota: Se l'etichetta degli account personali dell'organizzazione è stata rinominata, l'etichetta rinominata viene visualizzata nell'importazione guidata e nell'area degli strumenti della pagina iniziale degli account, ma non nella struttura di Imposta. Le etichette rinominate non appaiono in alcuna pagina di Imposta.

Eseguire le seguenti operazioni per importare gli account personali dell'organizzazione.

1. Avviare la procedura guidata a pagina 376
2. Evitare record duplicati a pagina 376
3. Specificare il titolare e le relazioni di ricerca
4. Selezionare il tipo di record a pagina 376
5. Caricare il file di importazione a pagina 377
6. Mappare i campi a pagina 377
7. Confermare e inviare la richiesta di importazione a pagina 377
8. Completare l'importazione a pagina 377

Nota: L'importazione guidata è dinamica; visualizza diverse schermate in base a quello che viene importato e all'impostazione dell'organizzazione.

## Avviare la procedura guidata

Per importare gli account personali dell'organizzazione:

1. Da Imposta, immettere "Importa account personali" nella casella `Ricerca veloce`, quindi selezionare **Importa account personali**.

   In alternativa, fare clic su **Importa account personali dell'organizzazione** nell'area degli strumenti della pagina iniziale Account.

2. Per ottenere risultati ottimali, eseguire tutte le operazioni indicate nella pagina introduttiva.
3. Fare clic su **Avviare l'importazione guidata** per iniziare l'importazione.

## Evitare record duplicati

1. L'importazione guidata è in grado di confrontare i record nel file di importazione con i record esistenti in Salesforce per impedire la creazione di record duplicati durante l'importazione. Specificare se si desidera impedire la creazione di record duplicati. Per aggiornare i record esistenti, è necessario selezionare `Sì`.
2. Se si sceglie `Sì` vengono visualizzate ulteriori opzioni:
   - Scegliere il campo da utilizzare per la ricerca di corrispondenze tra i record esistenti in Salesforce e i record nel file di importazione. L'opzione `ID esterno` è disabilitata se non è stato creato alcun campo di ID esterno per i record.
   - Specificare l'operazione da eseguire se vengono individuate corrispondenze: importare solo i nuovi record, aggiornare solo i record esistenti oppure aggiornare i record esistenti e importare quelli nuovi.

     Nota: Se si seleziona la ricerca di corrispondenze per `ID Salesforce`, è possibile solo aggiornare i record esistenti ma non importare quelli nuovi.

3. Fare clic su **Avanti**.

## Specificare il titolare e le relazioni di ricerca

1. Specificare il campo del file di importazione che contiene i titolari degli account personali.

   Quando si sceglie "Nome", sono validi i seguenti formati:

   - Nome seguito dal cognome
   - Cognome seguito dal nome
   - Alias
   - Nome utente

2. I record possono avere campi personalizzati che creano relazioni di ricerca con altri record. Se nel file di importazione sono stati inclusi campi di ricerca, selezionare le caselle corrispondenti.

   Nota: i record correlati devono essere già presenti in Salesforce prima di procedere. I record correlati non verranno aggiornati durante l'importazione, anche se il file di importazione contiene valori diversi per i campi presenti in tali record correlati.

3. Fare clic su **Avanti**.

## Selezionare il tipo di record

1. Scegliere il tipo di record che si desidera assegnare ai record nel file di importazione.
2. Se si inseriscono nuovi record e si aggiornano i record esistenti contemporaneamente, specificare se si desidera ignorare i tipi di record dei record esistenti.

3. Fare clic su **Avanti**.

## Caricare il file di importazione

1. Fare clic su **Sfoglia...** per specificare il percorso del file di importazione.
2. Selezionare la codifica dei caratteri del file di importazione. Nella maggior parte dei casi è possibile accettare il valore predefinito.
3. Specificare le impostazioni aggiuntive a seconda della configurazione dell'organizzazione, ad esempio se devono essere attivate le regole di flusso di lavoro e la lingua dei record nel file di importazione.
4. Fare clic su **Avanti**.

## Mappare i campi

1. Mappare i campi nel file di importazione con i campi appropriati di Salesforce ricercando la corrispondenza tra i campi sulla sinistra, che comprendono tutte le colonne del file di importazione, e il campo appropriato di Salesforce sulla destra. Se le etichette di colonna nel file di importazione corrispondono esattamente alle etichette di campo in Salesforce, tali campi verranno mappati automaticamente. Se invece due o più etichette di colonna del file corrispondono esattamente a un campo in Salesforce, tali campi dovranno essere mappati manualmente.

   Nota: Alcuni campi di Salesforce non possono essere aggiornati utilizzando l'importazione, ad esempio `Data creazione` e `Data ultima modifica`. Quindi, anche se si utilizza un rapporto esportato come file di importazione, alcuni campi di Salesforce nel file non potranno essere mappati.

2. Fare clic su **Avanti**. Se non sono stati mappati tutti i campi nel file di importazione, verrà visualizzato un avviso. I valori dei campi non mappati non vengono importati.

## Confermare e inviare la richiesta di importazione

1. Leggere tutti i messaggi di avviso visualizzati durante l'importazione guidata. Se lo si desidera, fare clic su **Indietro** per tornare a una fase precedente e risolvere eventuali problemi.
2. Scegliere **Importa ora** per inviare la richiesta di importazione a Salesforce.

## Completare l'importazione

1. Viene visualizzato un messaggio in cui è riportata la durata approssimativa dell'importazione. Al termine dell'operazione di importazione, verrà inviato un messaggio dell'Assistenza clienti all'indirizzo email visualizzato.
2. Fare clic su **Fine** per terminare la procedura guidata.
3. Per monitorare lo stato delle importazioni in sospeso, da Imposta, fare clic su **Monitoraggio** > **Importazioni**.

VEDERE ANCHE:

Importazione guidata dati

Creazione di file di esportazione per procedure di importazione

Preparazione dei dati per l'importazione

Panoramica sull'importazione

## Importazione guidata dati

Importazione guidata dati offre un'interfaccia unificata che consente di importare dati per numerosi oggetti Salesforce standard, inclusi account, referenti, lead e soluzioni. La procedura guidata consente anche di importare dati per gli oggetti personalizzati.

Importazione guidata dati consente di importare un massimo di 50.000 record contemporaneamente.

Salesforce consiglia di importare un piccolo file di prova per accertarsi che i dati di origine siano stati preparati correttamente.

La procedura Importazione guidata dati è supportata nei seguenti browser:

- Google Chrome™ versione 29 e successive
- Mozilla® Firefox® versione 23 e successive
- Microsoft® Internet Explorer® versione 9 e successive
- Apple® Safari® versione 5 e successive

La selezione con trascinamento dei file CSV non è supportata in Internet Explorer 9.

1. Preparare i dati per l'importazione e creare un file di importazione.

   Per evitare errori, duplicazione dei dati e altri problemi durante la preparazione dei dati per l'importazione prima di lanciare la procedura, si consiglia di consultare la Domanda frequente "Come si preparano i dati per l'importazione?" nella pagina di benvenuto di Importazione guidata dati.

2. Avviare la procedura guidata.
   a. Da Imposta, immettere *Importazione guidata dati* nella casella Ricerca veloce, quindi selezionare **Importazione guidata dati**.
   b. Rivedere le informazioni indicate nella pagina di benvenuto e fare clic su **Lancia l'importazione guidata!**

   Nota: Anche gli utenti che non sono amministratori possono accedere all'Importazione guidata dati delle proprie impostazioni personali.

3. Scegliere i dati che si desidera importare.
   a. Fare clic su **Oggetti standard** per importare account, referenti, lead o soluzioni. Fare clic su **Oggetti personalizzati** per importare oggetti personalizzati.
   b. Specificare se si desidera aggiungere nuovi record a Salesforce, aggiornare i record esistenti o aggiungere e aggiornare contemporaneamente i record.
   c. Specificare la corrispondenza e altri criteri secondo le esigenze. Passare il mouse sui punti interrogativi per ottenere ulteriori informazioni su ciascuna opzione.
   d. Specificare il file che contiene i dati.

      Per specificare il file di dati, trascinare il file CSV nell'area di caricamento della pagina oppure fare clic sulla categoria CSV che si sta utilizzando, quindi, andare al file e selezionarlo.
   e. Scegliere un metodo di codifica dei caratteri per il file. La maggior parte degli utenti non dovrà cambiare la codifica dei caratteri.
   f. Fare clic su **Avanti**.

4. Mappare i campi dati ai campi dati di Salesforce.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

AUTORIZZAZIONI UTENTE

Per importare account e referenti:
- "Importa referenti personali"

Per importare lead:
- "Importa lead"

Per importare le soluzioni:
- "Importa soluzioni"

Per importare oggetti personalizzati:
- "Modifica tutti i dati"

L'importazione guidata dati cerca di eseguire la mappatura del maggior numero possibile di campi dati con campi dati standard di Salesforce. Se Salesforce non riesce a mappare automaticamente i campi, sarà necessario farlo manualmente. I campi non mappati non vengono importati in Salesforce.

Per visualizzare un elenco di campi dati standard di Salesforce, dalle impostazioni di gestione per l'oggetto, passare all'area dei campi.

a. Analizzare l'elenco dei campi dati mappati e individuare i campi privi di mappatura.

b. Fare clic su **Mappa** a sinistra di ogni campo non mappato.

c. Nella finestra di dialogo Mappa il campo, scegliere il campo o i campi Salesforce da mappare e fare clic su **Mappa**.

Nota: la finestra di dialogo Mappa il campo consente inoltre di salvare i dati dei campi non mappati in un campo di note generali per account e referenti. Per eseguire questa operazione, scegliere Nota account o Nota referente dall'elenco a discesa Mappa a e fare clic su **Mappa**.

d. Per modificare le mappature che Salesforce ha eseguito automaticamente, fare clic su **Cambia** a sinistra del campo in questione, quindi scegliere il campo o i campi Salesforce da mappare e fare clic su **Mappa**.

e. Fare clic su **Avanti**.

5. Rivedere e avviare l'importazione.

a. Rivedere le informazioni sull'importazione nella pagina Esamina. Se vi sono ancora campi senza mappatura che si desidera importare, fare clic su **Precedente** per tornare alla pagina precedente e specificare le mappature.

b. Fare clic su **Avvia importazione**.

6. Controllare lo stato dell'importazione.

Da Imposta, digitare *Processi di caricamento dati in blocco* nella casella `Ricerca veloce`, quindi selezionare **Processi di caricamento dati in blocco**.

Nota: La pagina Processi di caricamento dati in blocco non è disponibile nella versione Professional Edition. Inoltre, solo gli amministratori hanno accesso alla pagina Processi di caricamento dati in blocco nella sezione Imposta di Salesforce. Se l'utente non è un amministratore, può verificare lo stato del caricamento monitorando le relative schede in Salesforce.

Per ricevere assistenza, accedere a www.salesforce.com/gettingstarted dove sono a disposizione webinar in diretta, video, procedure di configurazione e altro ancora. Per un aiuto concreto durante l'importazione dei dati, completare il modulo di importazione dei dati in Trailhead.

## Domande frequenti su Importazione guidata dati

- Quanti record è possibile importare?
- Quali tipi di oggetti è possibile importare?
- È possibile effettuare importazioni simultanee?
- Quanto tempo richiede un'importazione?

IN QUESTA SEZIONE:

Quanti record è possibile importare?

Quali tipi di oggetti è possibile importare?

È possibile effettuare importazioni simultanee?

Quanto tempo richiede un'importazione?

VEDERE ANCHE:

Importazione guidata dati

## Quanti record è possibile importare?

L'importazione guidata dei dati consente di importare fino a 50.000 record alla volta.

VEDERE ANCHE:

Domande frequenti su Importazione guidata dati

## Quali tipi di oggetti è possibile importare?

L'Importazione guidata dati consente di importare account, referenti, lead, soluzioni e oggetti personalizzati.

VEDERE ANCHE:

Domande frequenti su Importazione guidata dati

## È possibile effettuare importazioni simultanee?

L'Importazione guidata dati non supporta i processi di importazione dati simultanei. Prima di iniziare una nuova importazione è necessario avere completato quella precedente.

VEDERE ANCHE:

Domande frequenti su Importazione guidata dati

## Quanto tempo richiede un'importazione?

Il tempo richiesto per completare un'importazione mediante l'Importazione guidata dati varia a seconda della quantità di dati che si sta importando. Le importazioni, generalmente, non sono operazioni immediate e possono richiedere diversi minuti.

Se l'utente è un amministratore Salesforce, può verificare lo stato di un'importazione nella pagina dei download in blocco. Da Imposta, immettere *Processi di caricamento dati in blocco* nella casella Ricerca veloce, quindi selezionare **Processi di caricamento dati in blocco**.

Se l'utente non è un amministratore Salesforce, e desidera conoscere lo stato di un'importazione, dovrà aspettare di ricevere il messaggio email di stato. Inoltre, è possibile monitorare l'importazione manualmente controllando le relative schede in Salesforce.

VEDERE ANCHE:

Domande frequenti su Importazione guidata dati

# Utilizzo dell'area di attesa importazione

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

**Autorizzazioni utente richieste**

Per utilizzare l'area di attesa importazione:

- "Modifica tutti i dati"

Importante: Salesforce ha sostituito le singole procedure di importazione guidata per account, referenti e altri oggetti con una procedura unificata di Importazione guidata dati (le singole procedure di importazione guidata si aprono in piccole finestre popup, mentre l'importazione unificata si apre in un browser di dimensioni normali con dataimporter.app alla fine dell'URL). Per iniziare a utilizzare la procedura unificata, da Imposta, immettere *Importazione guidata dati* nella casella Ricerca veloce, quindi selezionare **Importazione guidata dati**. (le opzioni visualizzate dipendono dalle autorizzazioni di cui si dispone).

Gli amministratori possono controllare l'area di attesa importazione per visualizzare i dettagli di un'importazione o per annullare l'importazione di un'organizzazione. I dettagli delle importazioni vengono eliminati dall'area di attesa tre giorni dopo il termine dell'importazione.

1. Da Imposta, immettere *Importazioni* nella casella Ricerca veloce, quindi selezionare **Importazioni**.
2. Selezionare il nome del file di importazione per visualizzare la pagina Dettagli area di attesa importazione per quel file.

Se si desidera annullare un'importazione di cui non è ancora iniziata l'elaborazione, fare clic su **Canc**. Non è possibile annullare un'importazione una volta iniziata l'elaborazione.

Di seguito sono elencati i possibili valori della colonna Stato:

| Stato | Descrizione |
|---|---|
| Interrotto | L'importazione non è stata completata correttamente. I dettagli relativi agli errori vengono inviati per email all'utente che ha eseguito l'importazione. Se l'importazione si è interrotta è possibile ritentare entro tre giorni; tuttavia, se vengono fatti più tentativi, l'importazione non può rimanere nell'area di attesa per più di 30 giorni dal primo tentativo di importazione. |
| Completato | L'importazione è stata completata correttamente senza errori. |
| Errore | L'importazione è stata elaborata e si sono verificati degli errori. I dettagli relativi agli errori vengono inviati per email all'utente che ha eseguito l'importazione. L'utente può correggere gli errori e quindi riprovare a eseguire l'importazione. |
| In sospeso | L'importazione è nell'area di attesa ma l'elaborazione non è ancora iniziata. |
| Elaborazione in corso | L'importazione è nell'area di attesa ed è in corso di elaborazione. |

VEDERE ANCHE:

Importazione guidata dati

Panoramica sull'importazione

# Annullamento di un'importazione

Se si importano account, referenti, lead o soluzioni per errore, l'amministratore può, da Imposta, immettere `Eliminazione globale record` nella casella `Ricerca veloce`, quindi selezionare **Eliminazione globale record** per eliminare gli elementi importati per errore.

Gli strumenti Eliminazione globale record non supportano gli oggetti personalizzati. Se si importano erroneamente oggetti personalizzati nella versione Enterprise Edition, Unlimited Edition, Performance Edition o Developer Edition, l'amministratore può utilizzare Data Loader per l'eliminazione globale dei record importati per errore. Vedere Esecuzione di eliminazioni globali a pagina 395.

VEDERE ANCHE:

Importazione guidata dati

Panoramica sull'importazione

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

AUTORIZZAZIONI UTENTE

**Autorizzazioni utente richieste**

Per eliminare globalmente dati:

- "Modifica tutti i dati"

# Data Loader

## Data Loader

Data Loader è un'applicazione client per l'importazione o l'esportazione in massa di dati. È possibile utilizzarlo per inserire, aggiornare, eliminare o esportare record di Salesforce.

Durante l'importazione, Data Loader legge i dati, li estrae e li carica da file CSV o da una connessione al database. Anche l'esportazione avviene in file CSV.

Nota: se le virgole non sono appropriate per le proprie impostazioni internazionali, utilizzare la tabulazione o un altro delimitatore.

Data Loader può essere utilizzato in due modi:

- Interfaccia utente: quando si utilizza l'interfaccia utente, si lavora in modo interattivo per specificare i parametri della configurazione, i file CSV utilizzati per l'importazione e l'esportazione e le mappature dei campi che mappano i nomi dei campi nel file di importazione con i nomi dei campi in Salesforce.
- Riga di comando (solo Windows): quando si utilizza la riga di comando, si specificano la configurazione, le sorgenti di dati, le mappature e le azioni nei file. Questo consente di impostare Data Loader per l'elaborazione automatica.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Data Loader offre le seguenti funzionalità chiave:

- Interfaccia della procedura guidata facile e intuitiva per l'utilizzo interattivo
- Interfaccia alternativa dalla riga di comando per le operazioni in gruppi automatiche (solo Windows)
- Supporto per file di grandi dimensioni contenenti fino a 5 milioni di record
- Mappatura dei campi mediante trascinamento della selezione
- Supporto per tutti gli oggetti, anche personalizzati

- Può essere utilizzato per l'elaborazione dei dati sia in Salesforce sia in Database.com
- File di registro dettagliato per le operazioni riuscite e non riuscite in formato CSV
- Visualizzatore file CSV incorporato
- Supporto per Windows XP, Windows 7 e Mac OS X

Per iniziare, vedere i seguenti argomenti:

- Situazioni in cui è utile utilizzare Data Loader
- Installazione di Data Loader

Nota: nelle versioni precedenti Data Loader era denominato "AppExchange Data Loader" e "Sforce Data Loader".

VEDERE ANCHE:

Crittografia dei campi

Crittografia dei campi

## Situazioni in cui è utile utilizzare Data Loader

Data Loader funge da complemento per le funzionalità delle procedure guidate di importazione basate sul Web, accessibili dal menu Imposta nell'applicazione online. Per stabilire il metodo più appropriato per le proprie esigenze, tenere conto di quanto segue:

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

### Utilizzare Data Loader quando:

- È necessario caricare un numero di record compreso fra 50.000 e 5.000.000. Data Loader è supportato per caricare fino a 5 milioni di record. Se è necessario caricare più di 5 milioni di record, è consigliabile lavorare in collaborazione con un partner Salesforce o visitare il sito *App Exchange* per verificare la disponibilità di un prodotto partner adatto.
- È necessario caricare in un oggetto che non è ancora supportato dalle procedure guidate di importazione.
- Si desidera programmare caricamenti periodici di dati, ad esempio importazioni notturne.
- Si desidera esportare i dati per ragioni di backup.

### Utilizzare le procedure guidate di importazione quando:

- Si sta caricando un numero di record inferiore a 50.000.
- L'oggetto che si desidera importare è supportato dalle procedure guidate di importazione. Per visualizzare le procedure guidate di importazione disponibili e gli oggetti che supportano, da Imposta immettere *`Gestione dati`* nella casella `Ricerca veloce`, quindi selezionare **Gestione dati**.
- Si desidera impedire la creazione di duplicati caricando i record per nome e sito dell'account, indirizzo email del referente o indirizzo email del lead.

Per ulteriori informazioni sulle procedure guidate di importazione, vedere Panoramica sull'importazione a pagina 338.

# Installazione e configurazione di Data Loader

## Considerazioni per l'installazione di Data Loader

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per accedere alla pagina da cui scaricare Data Loader:

- "Modifica tutti i dati"

Per utilizzare Data Loader:

- Autorizzazione utente appropriata per l'operazione da eseguire, ad esempio "Crea" per gli account per inserire nuovi account

### Requisiti di sistema per Windows

Per utilizzare Data Loader per Windows è necessario disporre di:

- Microsoft® Windows® 7 o Windows XP
- 120 MB di spazio libero su disco
- 256 MB di memoria disponibile
- Java JRE 1.6
- Sun JVM 1.6
- Privilegi di amministratore per il computer

### Requisiti di sistema per Mac OS

Per utilizzare Data Loader per Mac è necessario disporre di:

- Mac® OS X
- 120 MB di spazio libero su disco
- 256 MB di memoria disponibile
- Java JRE 1.6
- Sun JVM 1.6
- Privilegi di amministratore per il computer

### Considerazioni sull'installazione

Con il passare del tempo, sono state messe a disposizione per il download numerose versioni dell'applicazione client Data Loader. Alcune delle versioni più datate erano denominate "AppExchange Data Loader" o "Sforce Data Loader". Sullo stesso computer è possibile eseguire diverse versioni contemporaneamente. Tuttavia, non installare più di una copia della stessa versione.

La versione più recente è sempre disponibile in Salesforce. Se è stata installata in precedenza la versione più recente e si desidera installarla di nuovo, rimuovere la versione in uso dal computer.

Suggerimento: se si verificano problemi di accesso nell'interfaccia della riga di comando dopo l'aggiornamento a una nuova versione di Data Loader, provare a crittografare nuovamente la password.

Nota: l'interfaccia della riga di comando di Data Loader è supportata solo per Windows.

Per apportare modifiche al codice sorgente, scaricare la versione open source di Data Loader da *https://github.com/forcedotcom/dataloader*.

### Considerazioni sull'accesso

Se l'organizzazione limita gli indirizzi IP, gli accessi da indirizzi IP non affidabili restano bloccati finché non vengono attivati. Salesforce invia automaticamente un messaggio email di attivazione che si può utilizzare per effettuare l'accesso. Il messaggio contiene un token di protezione da inserire alla fine della propria password. Ad esempio, se la password è `miapassword` e il token di protezione è *XXXXXXXXXX* è necessario immettere `miapassword`*XXXXXXXXXX* per accedere.

## Configurazione di Data Loader

È possibile modificare le impostazioni predefinite per il funzionamento di Data Loader.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

1. Aprire Data Loader.
2. Scegliere **Impostazioni** > **Impostazioni**.
3. Modificare i campi secondo le proprie necessità:

| Campo | Descrizione |
|---|---|
| `Batch size` | In un'unica operazione di inserimento, aggiornamento, inserimento con aggiornamento ed eliminazione, i movimenti di record da o a Salesforce vengono elaborati in incrementi di queste dimensioni. Il valore massimo è 200. Si consiglia di utilizzare un valore compreso tra 50 e 100.<br>Se è selezionata l'opzione `Use Bulk API`, il valore massimo è 10.000. |
| `Insert null values` | Selezionare questa opzione per inserire i valori mappati vuoti come valori `null` durante le operazioni sui dati. Tenere presente che, durante l'aggiornamento dei record, questa opzione trasmetterà a Data Loader l'istruzione di sovrascrivere i dati esistenti nei campi mappati.<br>Questa opzione non è disponibile se è selezionata l'opzione `Use Bulk API`. I valori dei campi vuoti vengono ignorati quando si aggiornano i record mediante l'API in blocco. Per impostare il valore di un campo su `null` quando è selezionata l'opzione `Use Bulk API`, utilizzare il valore di campo `#N/D`. |
| `Assignment rule` | Specificare l'ID della regola di assegnazione da utilizzare per inserimenti, aggiornamenti e inserimenti con aggiornamento. Questa opzione è valida per gli inserimenti, gli aggiornamenti e gli inserimenti con aggiornamento di casi e lead. È valida inoltre per gli aggiornamenti degli account se l'organizzazione dispone di regole di assegnazione dei territori per gli account. La regola di assegnazione sovrascrive i valori `Owner` nel file CSV. |
| `Server host` | Immettere l'URL del server Salesforce con cui si desidera comunicare. Ad esempio, se si |

| Campo | Descrizione |
| --- | --- |
| | stanno caricando dati in un Sandbox, l'URL in `https://test.salesforce.com`. |
| `Reset URL on Login` | Per impostazione predefinita, Salesforce reimposta l'URL dopo aver effettuato l'accesso a quello specificato nel `Server host`. Per disattivare questa reimpostazione automatica, disabilitare questa opzione. |
| `Compression` | L'opzione di compressione migliora le prestazioni di Data Loader ed è attivata per impostazione predefinita. Se è necessario eseguire il debug dei messaggi SOAP (Simple Object Access Protocol) sottostanti, è consigliabile disabilitare la compressione. Per disattivare la compressione, abilitare questa opzione. |
| `Timeout` | Indica per quanti secondi Data Loader attende una risposta dal server prima di segnalare un errore per la richiesta. |
| `Query request size` | In un'unica operazione di esportazione o di query, i record vengono restituiti da Salesforce in incrementi di queste dimensioni. Il valore massimo è 2.000 record. Se si specifica un valore superiore, le prestazioni possono migliorare ma viene utilizzata più memoria sul client. |
| `Generate status files for exports` | Selezionare questa opzione per generare file di esiti positivi e di errori quando si esportano dati. |
| `Read all CSVs with UTF-8 encoding` | Selezionare questa opzione per fare in modo che i file vengano aperti con la codifica UTF-8 anche se sono stati salvati in un formato diverso. |
| `Write all CSVs with UTF-8 encoding` | Selezionare questa opzione per fare in modo che tutti i file vengano scritti mediante la codifica UTF-8. |
| `Use European date format` | Selezionare questa opzione se si desidera utilizzare i formati data `gg/MM/aaaa` e `gg/MM/aaaa HH:mm:ss`. |
| `Allow field truncation` | Selezionare questa opzione per fare in modo che i dati vengano troncati nei seguenti tipi di campi durante il caricamento dei dati in Salesforce: Email, Elenco di selezione a selezione multipla, Telefono, Elenco di selezione, Testo e Testo (crittografato).<br>In Data Loader versione 14.0 e precedenti, i valori di questi tipi di campi vengono troncati se troppo lunghi. In Data Loader versione 15.0 e successive, l'operazione di caricamento non viene eseguita se un valore specificato è troppo lungo.<br>La selezione di questa opzione consente di richiedere l'utilizzo del comportamento precedente, vale a dire del troncamento, invece del nuovo comportamento previsto nelle versioni 15.0 e successive di Data Loader. Questa opzione è selezionata per impostazione predefinita e non ha alcun effetto nelle versioni 14.0 e precedenti. |

| Campo | Descrizione |
| --- | --- |
| | Questa opzione non è disponibile se è selezionata l'opzione `Use Bulk API`. In tal caso, l'operazione di caricamento per la riga non riesce se è stato specificato un valore troppo grande per il campo. |
| `Use Bulk API` | Selezionare questa opzione per utilizzare l'API in blocco per inserire, aggiornare, inserire con aggiornamento, eliminare ed eliminare definitivamente i record. L'API in blocco è ottimizzata in modo da caricare o eliminare un numero elevato di record in modo asincrono ed è più rapida dell'API basata su SOAP predefinita grazie all'elaborazione parallela e al minor numero di viaggi di andata e ritorno nella rete.<br><br>Avvertenza: quando si configura Data Loader con `Use Bulk API`, è possibile eliminare definitivamente dei record. Tenere presente che i record eliminati definitivamente vengono eliminati immediatamente e non possono essere recuperati dal Cestino. |
| `Enable serial mode for Bulk API` | Selezionare questa opzione per utilizzare l'elaborazione seriale anziché quella parallela per l'API in blocco. L'elaborazione in parallelo può causare conflitti per l'uso del database. Nei casi più gravi, il caricamento può non riuscire. L'utilizzo della modalità seriale fa sì che i batch vengano elaborati uno alla volta. Tenere presente che l'uso di questa opzione può incrementare in modo considerevole il tempo di elaborazione di un carico.<br><br>Questa opzione è disponibile solo se è selezionata l'opzione `Use Bulk API`. |
| `Upload Bulk API Batch as Zip File` | Selezionare questa opzione per utilizzare l'API in blocco per il caricamento di file zip contenenti allegati binari, ad esempio record Allegato o Salesforce CRM Content.<br><br>Questa opzione è disponibile solo se è selezionata l'opzione `Use Bulk API`. |
| `Time Zone` | Selezionare questa opzione per specificare un fuso orario predefinito.<br><br>Se il valore di una data non include il fuso orario, viene utilizzato questo valore.<br><br>• Se non è specificato alcun valore, viene utilizzato il fuso orario del computer in cui è installato Data Loader.<br>• Se è specificato un valore errato, viene utilizzato il fuso orario GMT e segnalato nel registro di Data Loader.<br><br>Sono validi tutti gli indicatori di fuso orario che possono essere passati al metodo `getTimeZone(java.lang.String)` Java. Il valore può essere costituito da un nome esteso, ad |

| Campo | Descrizione |
| --- | --- |
| | esempio `America/Los_Angeles`, o da un ID personalizzato, ad esempio `GMT-8:00`. |
| `Proxy host` | Il nome host del server proxy, quando applicabile. |
| `Proxy port` | La porta del server proxy. |
| `Proxy username` | Il nome utente per l'autenticazione del server proxy. |
| `Proxy password` | La password per l'autenticazione del server proxy. |
| `Proxy NTLM domain` | Il nome del dominio Windows utilizzato per l'autenticazione NTLM. |
| `Start at row` | Se l'ultima operazione non è riuscita, è possibile utilizzare questa impostazione per ricominciare dal punto in cui l'ultima operazione riuscita era stata terminata. |

4. Fare clic su **OK** per salvare le impostazioni.

VEDERE ANCHE:

Comportamento di Data Loader con l'API in blocco abilitata

Configurazione del Data Loader per utilizzare l'API in blocco

## Comportamento di Data Loader con l'API in blocco abilitata

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

L'abilitazione dell'API in blocco in Data Loader consente di caricare o eliminare un numero elevato di record più velocemente rispetto all'API predefinita basata su SOAP. Tuttavia vi sono alcune differenze di comportamento in Data Loader quando si abilita l'API in blocco. Una differenza importante è costituita dalla possibilità di eseguire l'eliminazione definitiva se si dispone dell'autorizzazione e della licenza. Vedere Configurazione di Data Loader a pagina 385.

Le impostazioni seguenti non sono disponibili nella pagina **Settings** > **Settings** di Data Loader quando è selezionata l'opzione `Use Bulk API`:

**`Insert null values`**
: Questa opzione consente a Data Loader di inserire valori mappati vuoti come valori `null` durante le operazioni sui dati quando l'API in blocco è disabilitata. I valori dei campi vuoti vengono ignorati quando si aggiornano i record mediante l'API in blocco. Per impostare il valore di un campo su `null` quando è selezionata l'opzione `Use Bulk API`, utilizzare il valore di campo `#N/D`.

**`Allow field truncation`**
: Questa opzione indica a Data Loader di troncare i dati per determinati tipi di campi quando l'API in blocco è disabilitata. Un'operazione di caricamento per la riga non riesce se viene specificato un valore troppo alto per il campo quando è selezionata l'opzione `Use Bulk API`.

VEDERE ANCHE:

Configurazione di Data Loader

## Configurazione del Data Loader per utilizzare l'API in blocco

L'API in blocco è ottimizzata in modo da caricare o eliminare un numero elevato di record in modo asincrono ed è più rapida dell'API basata su SOAP grazie all'elaborazione parallela e al minor numero di viaggi di andata e ritorno nella rete. Per impostazione predefinita, il Data Loader utilizza l'API basata su SOAP per elaborare i record.

Per configurare il Data Loader in modo da utilizzare l'API in blocco per inserire, aggiornare, inserire con aggiornamento, eliminare ed eliminare in modo definitivo i record:

1. Aprire Data Loader.
2. Scegliere **Impostazioni** > **Impostazioni**.
3. Selezionare l'opzione `Usa API in blocco`.
4. Fare clic su **OK**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Nota:

- È anche possibile selezionare l'opzione `Enable serial mode for Bulk API`. L'elaborazione in parallelo può causare conflitti per l'uso del database. Nei casi più gravi, il caricamento può non riuscire. L'utilizzo della modalità seriale fa sì che i batch vengano elaborati uno alla volta. Tenere presente che l'uso di questa opzione può incrementare in modo considerevole il tempo di elaborazione di un carico.
- **Attenzione:** È possibile eliminare definitivamente i record quando si configura l'opzione `Use Bulk API` in Data Loader. Tenere presente che i record eliminati definitivamente vengono eliminati immediatamente e non possono essere recuperati dal Cestino.

VEDERE ANCHE:

Configurazione di Data Loader

# Utilizzo di Data Loader

## Tipi di dati supportati da Data Loader

Data Loader supporta i seguenti tipi di dati:

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

**Base64**

Percorso stringa a file (converte il file nella matrice di caratteri con codifica base64). I campi base64 sono utilizzati solo per inserire o aggiornare gli allegati e Salesforce CRM Content. Per ulteriori informazioni, vedere Caricamento degli allegati a pagina 395 e Caricamento di contenuti con Data Loader a pagina 396.

**Booleano**

- Valori Vero (senza distinzione tra maiuscole e minuscole) = `yes`, `y`, `true`, `on`, `1`
- Valori Falso (senza distinzione tra maiuscole e minuscole) = `no`, `n`, `false`, `off`, `0`

**Formati di data**

Si consiglia di specificare le date nel formato *`aaaa-MM-ggTHH:mm:ss.SSS+/-HHmm`*:

- `aaaa` rappresenta l'anno a quattro cifre
- `MM` rappresenta il mese a due cifre (01-12)
- `gg` rappresenta il giorno a due cifre (01-31)

- `HH` rappresenta l'ora a due cifre (00-23)
- `mm` rappresenta il minuto a due cifre (00-59)
- `ss` rappresenta i secondi a due cifre (00-59)
- `SSS` rappresenta i millisecondi a tre cifre (000-999)
- `+/-HHmm` rappresenta il fuso orario UTC (Tempo coordinato universale)

Sono inoltre supportati i seguenti formati di data:

- `aaaa-MM-gg'T'HH:mm:ss.SSS'Z'`
- `aaaa-MM-gg'T'HH:mm:ss.SSS Pacific Standard Time`
- `aaaa-MM-gg'T'HH:mm:ss.SSSPacific Standard Time`
- `aaaa-MM-gg'T'HH:mm:ss.SSS PST`
- `aaaa-MM-gg'T'HH:mm:ss.SSSPST`
- `aaaa-MM-gg'T'HH:mm:ss.SSS GMT-08:00`
- `aaaa-MM-gg'T'HH:mm:ss.SSSGMT-08:00`
- `aaaa-MM-gg'T'HH:mm:ss.SSS-800`
- `aaaa-MM-gg'T'HH:mm:ss.SSS-800`
- `aaaa-MM-gg'T'HH:mm:ss`
- `aaaa-MM-gg HH:mm:ss`
- `aaaaMMgg'T'HH:mm:ss`
- `aaaa-MM-gg`
- `MM/gg/aaaa HH:mm:ss`
- `MM/gg/aaaa`
- `aaaaMMgg`

Tenere presenti i seguenti suggerimenti per i formati di data:

- Per abilitare i formati di data che iniziano con il giorno invece che con il mese, selezionare la casella `Use European date format` nella finestra di dialogo Impostazioni. I formati di data europei sono `gg/MM/aaaa` e `gg/MM/aaaa HH:mm:ss`.
- Se le impostazioni internazionali del computer specificano un fuso orario a est dell'Ora di Greenwich (GMT), si consiglia di modificare l'impostazione su GMT per evitare regolazioni della data quando si inseriscono o aggiornano record.
- Sono valide solo date che rientrano all'interno di un dato intervallo. La prima data valida è 1700-01-01T00:00:00Z GMT o appena dopo mezzanotte del 1 gennaio 1700. L'ultima data valida è 4000-12-31T00:00:00Z GMT o appena dopo mezzanotte del 31 dicembre 4000. Questi valori vengono aggiustati in base al fuso orario dell'utente. Ad esempio nel fuso orario del Pacifico la prima data valida è 1699-12-31T16:00:00 o le 16:00 del 31 dicembre 1699.

**Double**

Stringa Double standard

**ID**

Un ID di Salesforce è una stringa alfanumerica di 15 caratteri (con distinzione fra maiuscole e minuscole) o una stringa alfanumerica di 18 caratteri (senza distinzione tra maiuscole e minuscole) che identifica in modo univoco un determinato record.

Suggerimento: per garantire la qualità dei dati, fare attenzione a immettere gli ID di Salesforce in Data Loader con le maiuscole e le minuscole corrette.

**Intero**

Stringa intero standard

**Stringa**

Tutte le stringhe XML valide; eventuali caratteri XML non validi vengono rimossi.

## Esportazione dati

È possibile utilizzare l'esportazione guidata di Data Loader per estrarre dati da qualsiasi oggetto Salesforce. Durante l'esportazione, è possibile specificare di includere (**Export All**) o escludere (**Export**) i record eliminati in modo non definitivo.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per esportare record:
- "Lettura" per i record

Per esportare tutti i record:
- "Lettura" per i record

1. Aprire Data Loader.
2. Fare clic su **Export** o **Export All**. Questi comandi sono presenti anche nel menu File.
3. Inserire il nome utente e la password di Salesforce. Fare clic su **Log in** per accedere. Una volta completato l'accesso, scegliere **Next**. Non verrà richiesto di ripetere l'accesso fino alla disconnessione o chiusura del programma.

   Se l'organizzazione limita gli indirizzi IP, gli accessi da indirizzi IP non affidabili restano bloccati finché non vengono attivati. Salesforce invia automaticamente un messaggio email di attivazione che si può utilizzare per effettuare l'accesso. Il messaggio contiene un token di protezione da inserire alla fine della propria password. Ad esempio, se la password è `miapassword` e il token di protezione è `XXXXXXXXXX` è necessario immettere `miapasswordXXXXXXXXXX` per accedere.

4. Scegliere un oggetto. Ad esempio, selezionare l'oggetto Account. Se il nome dell'oggetto non è visualizzato nell'elenco predefinito, selezionare `Show all objects` per visualizzare un elenco completo di oggetti a cui è possibile accedere. Gli oggetti verranno elencati in base al nome di etichetta localizzato, con il nome dello sviluppatore indicato tra parentesi. Per le descrizioni degli oggetti, vedere *SOAP API Developer's Guide*.
5. Fare clic su **Browse...** per selezionare il file CSV in cui verranno esportati i dati. È possibile immettere un nuovo nome file per creare un nuovo file, oppure scegliere un file esistente.

   Se si seleziona un file esistente, il contenuto di tale file viene sostituito. Fare clic su **Sì** per confermare questa azione, oppure fare clic su **No** per scegliere un altro file.

6. Fare clic su **Avanti**.
7. Creare una query SOQL per l'esportazione dei dati. Ad esempio, selezionare `ID e Nome` nei campi della query e fare clic su **Fine**. Proseguendo con le procedure seguenti, si noterà che il visualizzatore CSV visualizza tutti i nomi Account e i rispettivi ID. SOQL (Salesforce Object Query Language) è il linguaggio Salesforce che consente di costruire stringhe di query semplici ma potenti. Analogamente al comando SELECT in SQL, SOQL consente di specificare l'oggetto di origine, un elenco di campi da recuperare e le condizioni per la selezione delle righe nell'oggetto di origine.
   a. Scegliere i campi da esportare.
   b. Se lo si desidera, selezionare le condizioni per il filtraggio del set di dati. Se non si seleziona alcuna condizione, verranno restituiti tutti i dati per i quali si dispone di accesso in lettura.
   c. Rivedere la query generata e apportare le modifiche eventualmente necessarie.

   Suggerimento: è possibile utilizzare una query di relazione SOQL per includere i campi da un oggetto correlato. Ad esempio:

```
Select Name, Pricebook2Id, Pricebook2.Name, Product2Id, Product2.ProductCode FROM
PricebookEntry WHERE IsActive = true
```

Oppure:

```
Select Id, LastName, Account.Name FROM Contact
```

Quando si utilizzano le query di relazione in Data Loader, i nomi dei campi specificati per intero distinguono le maiuscole dalle minuscole. Ad esempio, l'utilizzo di `ACCOUNT.NAME` anziché `Account.Name` non funziona.

Data Loader non supporta le query nidificate o che interrogano gli oggetti secondari. Ad esempio, le query simili a quella che segue restituiscono un errore:

```
SELECT Amount, Id, Name, (SELECT Quantity, ListPrice,
PriceBookEntry.UnitPrice, PricebookEntry.Name,
PricebookEntry.product2.Family FROM OpportunityLineItems)
FROM Opportunity
```

Inoltre, Data Loader non supporta le query che utilizzano relazioni polimorfiche. Ad esempio, la query seguente genera un errore:

```
SELECT Id, Owner.Name, Owner.Type, Owner.Id, Subject FROM Case
```

Per ulteriori informazioni su SOQL, vedere la guida *Force.com SOQL and SOSL Reference*.

8. Fare clic su **Finish**, quindi su **Yes** per confermare.
9. Viene visualizzata una finestra di informazioni sull'avanzamento nella quale è indicato lo stato dell'operazione.
10. Al termine dell'operazione viene visualizzata una finestra di conferma con il riepilogo dei risultati. Fare clic su **View Extraction** per visualizzare il file CSV oppure scegliere **OK** per chiudere la finestra. Per maggiori dettagli, vedere Revisione dei file di output di Data Loader a pagina 397.

Nota:

- Data Loader attualmente non supporta l'estrazione di allegati. Per risolvere il problema, si consiglia di utilizzare la funzione di esportazione settimanale nell'applicazione in linea per esportare gli allegati.
- Se si selezionano dei campi composti per l'esportazione in Data Loader, questi possono generare dei messaggi di errore. Utilizzare componenti di campi singoli per esportare i valori.

## Definizione delle mappature dei campi di Data Loader

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Per gli inserimenti, le eliminazioni o gli aggiornamenti di file, utilizzare la finestra di dialogo Mapping (Mappatura) per associare i campi di Salesforce alle colonne del file CSV. Per ulteriori informazioni, vedere Inserimento, aggiornamento o eliminazione di dati utilizzando Data Loader a pagina 393.

1. Per l'associazione automatica dei campi alle colonne, fare clic su **Auto-Match Fields to Columns** (Associa automaticamente i campi alle colonne). Data Loader compila l'elenco nella parte inferiore della finestra, in base alla similarità dei nomi di campi e colonne. Per un'operazione di eliminazione, la corrispondenza automatica funziona solo per il campo ID.
2. Per mappare manualmente i campi alle colonne, selezionare e trascinare i campi dall'elenco di campi Salesforce nella parte superiore dell'elenco di nomi delle intestazioni di colonna CSV situato nella parte inferiore. Ad esempio, se si stanno inserendo nuovi record Account dove il file CSV contiene i nomi di nuovi account, fare clic e trascinare il campo `Nome` a destra del campo dell'intestazione di colonna `NOME`.
3. Se si desidera, fare clic su **Save Mapping** (Salva mappatura) per salvare la mappatura per uso futuro. Specificare un nome per il file di mappatura SDL.

Se si seleziona un file esistente, il contenuto di tale file viene sostituito. Fare clic su **Yes** (Sì) per confermare questa azione, oppure fare clic su **No** per scegliere un altro file.

4. Per utilizzare la mappatura per l'operazione corrente, fare clic su **OK**.

## Inserimento, aggiornamento o eliminazione di dati con Data Loader

| AUTORIZZAZIONI UTENTE | |
|---|---|
| Per insert (inserire) i record: | "Crea" per il record |
| Per update (aggiornare) i record: | "Modifica" per il record |
| Per upsert (aggiornare e inserire) i record: | "Crea" o "Modifica" per il record |
| Per delete (eliminare) i record: | "Elimina" per il record |
| Per hard delete (eliminare definitivamente) i record: | "Elimina" per il record |

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Le procedure guidate per insert (inserimento), update (aggiornamento), upsert (inserimento con aggiornamento), delete (eliminazione) e hard delete (eliminazione definitiva) in Data Loader consentono di aggiungere nuovi record e di modificare o eliminare quelli esistenti. Tenere presente che "upsert" ("inserimento con aggiornamento") è una combinazione tra inserimento e aggiornamento. Se un record contenuto nel file corrisponde a un record esistente, il record esistente viene aggiornato con i valori presenti nel file. Se non viene trovata alcuna corrispondenza, viene creato un nuovo record. Quando si eliminano definitivamente i record, i record eliminati non vengono spostati nel Cestino e sono immediatamente disponibili per l'eliminazione. Per ulteriori informazioni, vedere Configurazione di Data Loader a pagina 385.

1. Aprire Data Loader.
2. Fare clic su **Insert** (Inserisci), **Update** (Aggiorna), **Upsert** (Aggiorna e inserisci) , **Delete** (Elimina) o **Hard Delete** (Elimina definitivamente). Questi comandi sono presenti anche nel menu File (File).
3. Inserire il nome utente e la password di Salesforce. Fare clic su **Log in** (Accedi) per accedere. Una volta completato l'accesso, scegliere **Next** (Avanti). Non verrà richiesto di ripetere l'accesso fino alla disconnessione o chiusura del programma.

   Se l'organizzazione limita gli indirizzi IP, gli accessi da indirizzi IP non affidabili restano bloccati finché non vengono attivati. Salesforce invia automaticamente un messaggio email di attivazione che si può utilizzare per effettuare l'accesso. Il messaggio contiene un token di protezione da inserire alla fine della propria password. Ad esempio, se la password è `miapassword` e il token di protezione è `XXXXXXXXXX` è necessario immettere `miapasswordXXXXXXXXXX` per accedere.

4. Scegliere un oggetto. Ad esempio, se si stanno inserendo dei record di account, selezionare **Account**. Se il nome dell'oggetto non è visualizzato nell'elenco predefinito, selezionare `Show all objects` per visualizzare un elenco completo di oggetti a cui è possibile accedere. Gli oggetti vengono elencati in base al nome di etichetta localizzato, con il nome dello sviluppatore indicato tra parentesi. Per le descrizioni degli oggetti, vedere *Riferimento oggetti per Salesforce e Force.com*.
5. Fare clic su **Browse...** (Sfoglia) per selezionare il file CSV. Ad esempio, se si stanno inserendo record di account, è possibile specificare un file CSV di nome `insertaccounts.csv` contenente una colonna `Nome` per i nomi dei nuovi account.
6. Fare clic su **Next** (Avanti). Dopo l'inizializzazione dell'oggetto e del file CSV, scegliere **OK**.
7. Se si sta eseguendo un inserimento con aggiornamento (upsert):
   a. Il file CSV deve contenere una colonna di valori ID di cui individuare la corrispondenza con record esistenti. La colonna può essere un ID esterno (un campo personalizzato che possiede l'attributo "ID esterno") o `Id` (l'ID record Salesforce). Dall'elenco a discesa

scegliere il file da utilizzare per la corrispondenza. Se l'oggetto non ha campi con ID esterni, viene utilizzato automaticamente `Id`. Fare clic su **Next** (Avanti) per continuare.

b. Se il file comprende gli ID esterni di un oggetto che detiene una relazione con l'oggetto scelto, abilitare quell'ID esterno per individuare la corrispondenza tra i record selezionandone il nome dall'elenco a discesa. Se in questa fase non viene eseguita alcuna selezione, è possibile utilizzare il campo `Id` dell'oggetto correlato per la corrispondenza mappandolo nella fase successiva. Fare clic su **Next** (Avanti) per continuare.

8. Definire la mappatura delle colonne nel file CSV con i campi di Salesforce. Fare clic su **Choose an Existing Map** (Scegli una mappa esistente) per selezionare una mappatura di campi esistente oppure fare clic su **Create or Edit a Map** (Crea o modifica una mappa) per crearne una nuova o modificarne una esistente. Per ulteriori informazioni e un esempio dell'utilizzo, vedere Definizione delle mappature dei campi di Data Loader a pagina 392.
9. Fare clic su **Next** (Avanti).
10. Per ogni operazione, Data Loader genera due file di registro univoci in formato CSV, il cui nome file inizia con “success” per il primo ed “error” per il secondo. Fare clic su **Browse...** (Sfoglia) per specificare una directory per tali file.
11. Fare clic su **Finish** (Fine) per eseguire l'operazione, quindi scegliere **Yes** (Sì) per confermare.
12. Nel corso dell'operazione viene visualizzata una finestra di informazioni sull'avanzamento nella quale è indicato lo stato del trasferimento dei dati.
13. Al termine dell'operazione viene visualizzata una finestra di conferma con il riepilogo dei risultati. Fare clic su **View Successes** (Visualizza successi) per visualizzare il file di esiti positivi e su **View Errors** (Visualizza errori) per aprire il file degli errori oppure scegliere **OK** per chiudere. Per ulteriori informazioni, vedere Revisione dei file di output di Data Loader a pagina 397.

Suggerimento:

- In caso di aggiornamento o eliminazione di grandi quantità di dati, rivedere Esecuzione di aggiornamenti globali ed Esecuzione di eliminazioni globali per suggerimenti e procedure consigliate.
- Viene imposto un limite di cinque minuti sull'elaborazione di 100 record quando è abilitata l'API in blocco. Inoltre, se l'elaborazione di un file richiede più di 10 minuti, l'API in blocco rimette in coda la parte rimanente del file per un'elaborazione successiva. Se l'API in blocco continua a superare il limite di 10 minuti nei successivi tentativi, il file viene rimesso in coda e rielaborato un massimo di 10 volte prima che l'operazione venga definitivamente contrassegnata come non riuscita. È possibile tuttavia che anche se l'elaborazione non è riuscita alcuni record siano stati completati. Per questa ragione, è necessario verificare i risultati. Se viene visualizzato un errore di timeout durante il caricamento di un file, suddividerlo in vari file più piccoli e riprovare.

## Esecuzione di aggiornamenti globali

Per aggiornare contemporaneamente un gran numero di record, si raccomanda la seguente procedura:

1. Procurarsi i dati esportando gli oggetti da aggiornare o eseguendo un rapporto. Assicurarsi che il rapporto includa l'ID dei record.
2. Come misura di backup, salvare una copia aggiuntiva del file CSV generato.
3. Aprire il file di lavoro in un editor CSV come Excel e aggiornare i dati.
4. Avviare Data Loader e seguire le istruzioni dell'aggiornamento guidato. Tenere presente che l'associazione viene effettuata in base all'ID dei record. Vedere Inserimento, aggiornamento o eliminazione di dati utilizzando Data Loader a pagina 393.
5. Al termine, rivedere i file di registro “success” ed “error”. Vedere Revisione dei file di output di Data Loader a pagina 397.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

6. Se si commette un errore, utilizzare il file di backup per ripristinare i record ai valori precedenti.

## Esecuzione di eliminazioni globali

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Per eliminare contemporaneamente un elevato numero di record utilizzando Data Loader, si consiglia la seguente procedura:

1. Come precauzione, esportare i record da eliminare, accertandosi di selezionare tutti i campi (vedere Esportazione dei dati a pagina 391). Salvare una copia aggiuntiva del file CSV generato.
2. Esportare quindi i record da eliminare, utilizzando questa volta come criterio solo l'ID record.
3. Avviare Data Loader e seguire le istruzioni dell'eliminazione o eliminazione definitiva guidata. Mappare solo la colonna ID. Vedere Inserimento, aggiornamento o eliminazione di dati utilizzando Data Loader a pagina 393.
4. Al termine, rivedere i file di registro “success” ed “error”. Vedere Revisione dei file di output di Data Loader a pagina 397.

## Caricamento di allegati

Data Loader consente di caricare allegati in Salesforce. Prima di caricare gli allegati, tenere presente quanto segue:

- Se si intende eseguire il caricamento mediante l'API in blocco, verificare che l'opzione `Upload Bulk API Batch as Zip File` nella pagina **Settings** > **Settings** sia abilitata.
- Per eseguire la migrazione di allegati da un'organizzazione Salesforce di origine a un'organizzazione Salesforce di destinazione, iniziare richiedendo un'esportazione di dati per l'organizzazione di origine. Nella pagina Pianifica esportazione, assicurarsi di selezionare la casella di controllo `Includi allegati...` che include il file `Attachment.csv` nell'esportazione. Questo file CSV può essere utilizzato per caricare gli allegati. Per ulteriori informazioni sul servizio di esportazione, vedere Esportazione di dati di backup a pagina 437.

Per caricare gli allegati:

1. Confermare che il file CSV che si desidera utilizzare per l'importazione degli allegati include le seguenti colonne (ogni colonna rappresenta un campo di Salesforce):
   - `ParentId`: ID Salesforce del record controllante.
   - `Name`: nome del file allegato, ad esempio `mioallegato.jpg`.
   - `Body`: il percorso assoluto all'allegato sull'unità locale.

     Verificare che i valori della colonna `Body` contengano il nome completo degli allegati presenti nel computer. Ad esempio, se un allegato denominato `myattachment.jpg` si trova sul computer in `C:\Export`, `Body` deve specificare `C:\Export\myattachment.jpg`. Il file CSV potrebbe avere l'aspetto seguente:

     ```
     ParentId,Name,Body
     50030000000VDowAAG,attachment1.jpg,C:\Export\attachment1.gif
     701300000000iNHAAY,attachment2.doc,C:\Export\files\attachment2.doc
     ```

   Il file CSV può anche includere altri campi Allegato opzionali, quali `Description`.

2. Procedere con l'operazione di inserimento o inserimento con aggiornamento; vedere Inserimento, aggiornamento o eliminazione di dati utilizzando Data Loader a pagina 393. Nella fase `Select data objects`, assicurarsi di selezionare la casella di controllo `Show all Salesforce objects` e il nome oggetto `Attachment` nell'elenco.

## Caricamento di contenuti con Data Loader

È possibile utilizzare Data Loader per caricare in blocco documenti e link nelle librerie di Salesforce CRM Content. Prima di caricare documenti o link, tenere presente quanto segue:

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

- Se si intende eseguire il caricamento mediante l'API in blocco, verificare che l'opzione `Upload Bulk API Batch as Zip File` nella pagina **Settings** > **Settings** sia abilitata.
- Quando si carica un documento dall'unità locale utilizzando Data Loader, specificare il percorso nei campi `VersionData` e `PathOnClient` nel file CSV. `VersionData` identifica la posizione ed estrae il formato, mentre `PathOnClient` identifica il tipo di documento che viene caricato.
- Quando si carica un link utilizzando Data Loader, specificare l'URL in `ContentUrl`. Non utilizzare `PathOnClient` o `VersionData` per caricare i link.
- Non è possibile esportare contenuti utilizzando Data Loader.
- Se si stanno aggiornando contenuti già caricati:
  - Eseguire la funzione insert.
  - Includere una colonna `ContentDocumentId` con un ID di 18 caratteri. Salesforce utilizza queste informazioni per determinare che si stanno aggiornando i contenuti. Quando si esegue la mappatura di `ContentDocumentId`, gli aggiornamenti vengono aggiunti al file dei contenuti. Se non si include ContentDocumentId, i contenuti vengono considerati nuovi e il file dei contenuti non viene aggiornato.

1. Creare un file CSV con i campi seguenti.
   - `Title` - nome del file.
   - `Description` - (facoltativo) descrizione del file o del link.

     Nota: Se la descrizione contiene virgole, utilizzare le virgolette doppie attorno al testo.

   - `VersionData` - percorso completo del file sull'unità locale (solo per caricare i documenti).

     Nota: I file vengono convertiti nella codifica base64 durante il caricamento, L'azione aumenta la dimensione del file di circa il 30%.

   - `PathOnClient` - percorso completo del file sull'unità locale (solo per caricare i documenti).
   - `ContentUrl` - URL (solo per caricare i link).
   - `OwnerId` - (facoltativo) proprietario del file, l'impostazione predefinita è l'utente che sta caricando il file.
   - `FirstPublishLocationId` - ID della libreria.
   - `RecordTypeId` - ID del tipo di record.

     Nota: se si pubblica in una libreria con tipi di record limitati, specificare `RecordTypeId`.

   Per determinare i valori `RecordTypeId` per la propria organizzazione utilizzando Data Loader, seguire le operazioni indicate in Esportazione di dati. Di seguito è riportato un esempio di query SOQL:

   ```
   Select Id, Name FROM RecordType WHERE SobjectType = 'ContentVersion'
   ```

   Per determinare i valori `RecordTypeId` per la propria organizzazione utilizzando il Toolkit AJAX:

   a. Accedere a Salesforce.

   b. Immettere questo URL nel browser: `http://`***`instanceName`***`.salesforce.com/soap/ajax/35.0/debugshell.html`. Immettere il valore

*instanceName*, ad esempio *na1*, per la propria organizzazione. *instanceName* è visibile nel campo URL del browser dopo l'accesso a Salesforce.

c. Nel tipo di pagina Toolkit AJAX Shell:

```
sforce.connection.describeSObject("ContentVersion")
```

d. Premere **Invio**.

e. Fare clic sulle frecce per `recordTypeInfos`.

Vengono elencati i valori `RecordTypeId` della propria organizzazione.

- `TagsCsv` - tag (facoltativo).

Un file CSV di esempio è:

```
Title,Description,VersionData,PathOnClient,OwnerId,FirstPublishLocationId,RecordTypeId,TagsCsv
testfile,"This is a test file, use for bulk
upload",c:\files\testfile.pdf,c:\files\testfile.pdf,005000000000000,058700000004Cd0,012300000008o2sAQG,one
```

2. Caricare il file CSV per l'oggetto ContentVersion (vedere Inserimento, aggiornamento o eliminazione di dati utilizzando Data Loader a pagina 393). Tutti i documenti e i link sono disponibili nella libreria specificata.

## Revisione dei file di output di Data Loader

Dopo ogni importazione o esportazione, Data Loader genera due file CSV di output che contengono i risultati dell'operazione. Un nome file inizia con “success”, mentre l'altro inizia con “error”. Durante ogni esportazione, Data Loader salva i dati estratti nel file CSV specificato nella procedura guidata. Data Loader dispone di un visualizzatore di file CSV incorporato che consente di aprire e visualizzare tali file.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Per visualizzare i file di output generati da un'operazione di Data Loader:

1. Scegliere **View (Visualizza)** > **View CSV (Visualizza CSV)**.
2. Specificare il numero di righe da visualizzare. Ogni riga del file CSV corrisponde a un record di Salesforce. Il valore predefinito è 1000.
3. Per visualizzare un file CSV, fare clic su **Open CSV (Apri CSV)**. Per visualizzare l'ultimo file “success”, fare clic su **Open Success (Apri Success)**. Per visualizzare l'ultimo file “error”, fare clic su **Open Error (Apri Error)**. Il file CSV viene aperto in una nuova finestra.
4. Se lo si desidera, fare clic su **Open in External Program (Apri in programma esterno)** per aprire il file nel programma esterno associato, ad esempio Microsoft® Office Excel.

   Il file “success” contiene tutti i record che sono stati caricati e include una colonna per gli ID record generati di recente. Il file “error” contiene tutti i record che sono stati rifiutati dall'operazione di caricamento e include una colonna che descrive il motivo del mancato caricamento.

5. Fare clic su **Close (Chiudi)** per ritornare alla finestra CSV Chooser (Selettore CSV), quindi fare clic su **OK** per uscire dalla finestra.

Nota: per generare file "success" quando si esportano i dati, selezionare l'impostazione `Generate status files for exports (Genera file di stato per le esportazioni)`. Per ulteriori informazioni, vedere Configurazione di Data Loader a pagina 385.

### Visualizzazione del file registro di Data Loader

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Se è necessario cercare la causa di un problema di Data Loader oppure quando viene richiesto dal servizio di Assistenza clienti di Salesforce, è possibile accedere ai file di registro che tengono traccia delle operazioni e delle connessioni di rete effettuate da Data Loader.

Il file di registro, `sdl.log`, contiene un elenco cronologico dettagliato delle voci del registro di Data Loader. Le voci di registro contrassegnate con "INFO" rappresentano elementi procedurali, come l'accesso e l'uscita da Salesforce. Le voci contrassegnate con "ERROR" rappresentano dei problemi come, ad esempio, un record inviato in cui manca un campo obbligatorio. Il file di registro può essere aperto mediante un normale editor di testo, come il Blocco note di Microsoft.

Se si utilizza Data Loader per Windows, visualizzare il file di registro immettendo *`%TEMP%\sdl.log`* nella finestra di dialogo Esegui o nella barra degli indirizzi di Esplora risorse.

Se si utilizza Data Loader per Mac OSX, visualizzare il file di registro aprendo il terminale e immettendo *`open $TMPDIR/sdl.log`*.

Se si verificano problemi di accesso dall'interfaccia utente, può essere necessario un nuovo token di protezione.

## Esecuzione dei processi in batch (solo Windows)

### Modalità a gruppi

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Nota: l'interfaccia della riga di comando di Data Loader è supportata solo per Windows.

È possibile eseguire Data Loader nella modalità a gruppi dalla riga di comando. Vedere i seguenti argomenti:

- Directory e file installati
- Crittografia dalla riga di comando
- Aggiornamento dell'interfaccia in modalità a gruppi
- Interfaccia della riga di comando di Data Loader
- Configurazione dei processi batch
- Parametri di configurazione dei processi Data Loader
- Operazioni dalla riga di comando di Data Loader
- Configurazione dell'accesso al database
- Mappatura di colonne
- Esecuzione di processi batch singoli
- Oggetti di accesso ai dati

Nota: Se è stata utilizzata la modalità a gruppi dalla riga di comando con una versione precedente alla 8.0, vedere Aggiornamento dell'interfaccia in modalità a gruppi a pagina 400.

## Directory e file installati

Nota: l'interfaccia della riga di comando di Data Loader è supportata solo per Windows.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Nella versione 8.0 e nelle versioni successive, l'installazione di Data Loader crea diverse directory nella directory di installazione. Le seguenti directory vengono utilizzate per l'esecuzione del programma dalla riga di comando per l'elaborazione batch automatica:

**bin**

Include i file batch `encrypt.bat` per la crittografia delle password e `process.bat` per l'esecuzione di processi batch.

Per informazioni sull'esecuzione di Data Loader dalla riga di comando, vedere Interfaccia della riga di comando di Data Loader a pagina 400.

**conf**

Directory di configurazione predefinita. Contiene i file di configurazione `config.properties`, `Loader.class` e `log-conf.xml`.

Il percorso del file `config.properties` generato quando si modifica la finestra di dialogo Impostazioni nell'interfaccia utente grafica è `C:\Documenti\`*`nome utente di Windows`*`\Dati applicazioni\Salesforce\Data Loader` *`numero_versione`*. È possibile copiare il file nella directory di installazione `conf` per utilizzarlo per i processi batch.

**samples**

Contiene sottodirectory di file di esempio di riferimento.

### Convenzione dei percorsi file

I percorsi file specificati in questi argomenti iniziano da un livello inferiore alla directory di installazione. Ad esempio, `\bin` indica `C:\Programmi\Salesforce\Data Loader` *`numero_versione`*`\bin`, a condizione che sia stata accettata la directory di installazione predefinita. Se il programma è stato installato in un percorso diverso, specificare il percorso appropriato.

## Crittografia dalla riga di comando

Nota: l'interfaccia della riga di comando di Data Loader è supportata solo per Windows.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Quando si esegue Data Loader nella modalità a gruppi dalla riga di comando, è necessario crittografare i seguenti parametri di configurazione:

- `sfdc.password`
- `sfdc.proxyPassword`

Data Loader include un'utility di crittografia per proteggere le password specificate nei file di configurazione. L'utility viene utilizzata per crittografare le password, ma i dati trasmessi con Data Loader non vengono crittografati.

1. Eseguire `\bin\encrypt.bat`.
2. Dalla riga di comando, attenersi alle istruzioni visualizzate per eseguire le seguenti azioni:

   **Generazione di una chiave**

   Il testo della chiave viene generato sullo schermo in base al testo specificato. Copiare il testo della chiave in un file chiave, omettendo gli spazi iniziali o finali. Il file chiave potrà quindi essere utilizzato per la crittografia e la decrittografia.

**Crittografia di un testo**

Viene generata la versione crittografata di una password o di un altro testo. Se lo si desidera, è possibile fornire un file chiave per la crittografia. Nel file di configurazione, assicurarsi che il testo crittografato venga copiato correttamente e che il file chiave sia menzionato.

**Verifica del testo crittografato**

Dopo aver specificato le versioni crittografate e decrittografate di una password, viene verificato se la password crittografata corrisponde alla versione decrittografata. Nella riga di comando viene visualizzato un messaggio di operazione completata o non riuscita.

## Aggiornamento dell'interfaccia in modalità a gruppi

Nota: l'interfaccia della riga di comando di Data Loader è supportata solo per Windows.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

L'interfaccia in modalità a gruppi delle versioni di Data Loader 8.0 e successive non è compatibile con le versioni precedenti. Se si utilizza una versione precedente alla 8.0 per l'esecuzione di processi batch, è possibile:

**Mantenere la versione precedente per i processi batch**

Non disinstallare la versione precedente di Data Loader. Continuare a utilizzare questa versione per i processi batch. Non sarà possibile utilizzare le nuove funzioni, quale la connettività database, ma le integrazioni continueranno a funzionare. Se lo si desidera, installare la nuova versione mantenendo la versione precedente e utilizzare quest'ultima soltanto per i processi batch.

**Generare un nuovo file config.properties dalla nuova interfaccia utente grafica**

Se il file `config.properties` è stato generato dall'interfaccia utente grafica, utilizzare la nuova versione per impostare le stesse proprietà e generare un nuovo file. Utilizzare il nuovo file generato con la nuova interfaccia in modalità a gruppi.

**Aggiornare manualmente il file config.properties**

Se il file `config.properties` esistente è stato creato manualmente, sarà necessario aggiornarlo manualmente per la nuova versione. Per ulteriori informazioni, vedere Directory e file installati a pagina 399.

## Interfaccia della riga di comando di Data Loader

Nota: l'interfaccia della riga di comando di Data Loader è supportata solo per Windows.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Per le operazioni in gruppi (batch) automatiche, quali i caricamenti e le estrazioni pianificati per l'esecuzione notturna, eseguire Data Loader dalla riga di comando. Prima di eseguire qualsiasi operazione in gruppi, accertarsi di avere incluso la propria password crittografata nel file di configurazione. Per ulteriori informazioni, vedere Introduzione a Data Loader a pagina 418 e Crittografia dalla riga di comando a pagina 399. Dalla riga di comando, passare alla directory `bin` e digitare *`process.bat`*, che utilizza i seguenti parametri:

- La directory contenente `config.properties`.
- Il nome del bean del processo batch contenuto in `process-conf.xml`.

Per ulteriori informazioni sull'uso di *`process.bat`*, vedere Esecuzione di processi batch singoli a pagina 417.

Per visualizzare suggerimenti e istruzioni, aggiungere *`-help`* al comando contenuto in *`process.bat`*.

Data Loader verrà eseguito indipendentemente dall'operazione, file o mappa specificata nel file di configurazione indicato. Se non si specifica una directory di configurazione, viene utilizzata la directory corrente. Per impostazione predefinita, i file di configurazione di Data Loader vengono installati nella seguente cartella:

`C:\Programmi\Salesforce\Data Loader` *`numero versione`*`\conf`

Per configurare l'elaborazione batch si utilizza il file `process-conf.xml`. Impostare il nome del processo nell'attributo id dell'elemento bean: (ad esempio <bean id="NomeMioProcesso">).

Se si desidera implementare funzionalità di accesso avanzato, utilizzare un copia di `log-conf.xml`.

È possibile modificare i parametri in fase di esecuzione specificando *`param=value`* come argomenti del programma. Ad esempio, l'aggiunta di `process.operation=insert` al comando, determina la modifica della configurazione in fase di esecuzione.

Si possono impostare le dimensioni minime e massime dell'heap. Ad esempio, `-Xms256m -Xmx256m` imposta le dimensioni dell'heap su 256 MB.

Nota: questi argomenti sono validi solo per Data Loader versione 8.0 e successive.

Suggerimento: se si verificano problemi di accesso nell'interfaccia della riga di comando dopo l'aggiornamento a una nuova versione di Data Loader, provare a crittografare nuovamente la password.

## Configurazione dei processi batch

Nota: l'interfaccia della riga di comando di Data Loader è supportata solo per Windows.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Utilizzare `\samples\conf\process-conf.xml` per configurare i processi Data Loader rappresentati dai bean ProcessRunner. È necessario che per il processo venga specificato `ProcessRunner` come attributo `class` e che vengano impostate le seguenti proprietà nel file di configurazione:

**name**
: Imposta il nome del bean ProcessRunner. Questo valore viene utilizzato anche come nome di thread non generico e per i file di backup di configurazione (vedere di seguito).

**configOverrideMap**
: Proprietà di tipo `map` in cui ciascuna voce rappresenta un'impostazione di configurazione: la chiave corrisponde al nome dell'impostazione; il valore corrisponde al valore dell'impostazione.

**enableLastRunOutput**
: Se impostata su true (impostazione predefinita), i file di output contenenti informazioni sull'ultima esecuzione, ad esempio `sendAccountsFile_lastrun.properties`, vengono generati e salvati nel percorso specificato da `lastRunOutputDirectory`. Se impostata su false, i file non vengono generati o salvati.

**lastRunOutputDirectory**
: Percorso della directory in cui vengono scritti i file di output contenenti informazioni sull'ultima esecuzione, ad esempio `sendAccountsFile_lastrun.properties`. Il valore predefinito è `\conf`. Se `enableLastRunOutput` è impostata su false, il valore non viene utilizzato poiché i file non vengono generati.

Il file di backup di configurazione memorizza i valori dei parametri di configurazione dell'ultima esecuzione a scopo di debug e viene utilizzato per caricare i parametri di configurazione predefiniti in `config.properties`. Le impostazioni di `configOverrideMap` hanno la precedenza su quelle del file di backup di configurazione. Il file di backup di configurazione viene gestito a livello di programmazione e non richiede alcuna modifica manuale.

Per i nomi e le descrizioni dei parametri di configurazione dei processi disponibili, vedere Parametri di configurazione dei processi Data Loader a pagina 402.

## Parametri di configurazione dei processi Data Loader

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Nota: l'interfaccia della riga di comando di Data Loader è supportata solo per Windows.

Quando si esegue Data Loader dalla riga di comando, è possibile specificare i seguenti parametri di configurazione nel file `process-conf.xml`. In alcuni casi, il parametro è rappresentato anche nell'interfaccia grafica utente in **Impostazioni** > **Impostazioni**.

Suggerimento: un esempio di file `process-conf.xml` è disponibile nella directory `\samples` installata con Data Loader.

| Nome parametro | Tipo di dati | Opzione equivalente della finestra di dialogo Impostazioni | Descrizione |
|---|---|---|---|
| `dataAccess.readUTF8` | booleano | `Read all CSVs with UTF-8 encoding` | Selezionare questa opzione per fare in modo che i file vengano aperti con la codifica UTF-8 anche se sono stati salvati in un formato diverso.<br>Valore di esempio: `true` |
| `dataAccess.writeUTF8` | booleano | `Write all CSVs with UTF-8 encoding` | Selezionare questa opzione per fare in modo che i file vengano scritti mediante la codifica UTF-8.<br>Valore di esempio: `true` |
| `dataAccess.name` | stringa | Non applicabile (N/A) | Nome della fonte di dati da utilizzare, ad esempio il nome di un file CSV. Per i database, utilizzare il nome della configurazione di database in `database-conf.xml`.<br>Valore di esempio: `c:\dataloader\data\extractLead.csv` |
| `dataAccess.readBatchSize` | intero | N/D | Numero di record letti contemporaneamente dal database. Il valore massimo è 200.<br>Valore di esempio: `50` |
| `dataAccess.type` | stringa | N/D | Tipo di fonte di dati standard o personalizzato. I tipi standard sono `csvWriter`, `csvRead`, `databaseWrite` e `databaseRead`. |

| Nome parametro | Tipo di dati | Opzione equivalente della finestra di dialogo Impostazioni | Descrizione |
|---|---|---|---|
| | | | Valore di esempio: `csvWrite` |
| `dataAccess.writeBatchSize` | intero | N/D | Numero di record scritti contemporaneamente nel database. Il valore massimo è 2.000. Per i valori di parametro elevati, tenere presente quanto segue: se si verifica un errore, tutti i record del batch vengono ritirati. Al contrario, se il valore è impostato su 1, ogni record viene elaborato separatamente (non in gruppo) e gli errori sono specifici per quel record. Si consiglia di impostare il valore su 1 quando si desidera individuare i problemi di scrittura in un database.<br>Valore di esempio: `500` |
| `process.enableExtractStatusOutput` | booleano | `Generate status files for exports` | Selezionare questa opzione per generare file di esiti positivi e di errori quando si esportano dati.<br>Valore di esempio: `true` |
| `process.enableLastRunOutput` | booleano | N/D | Quando si esegue Data Loader nella modalità gruppi è possibile disabilitare la generazione di file di output, ad esempio `sendAccountsFile_lastRun.properties`. Per impostazione predefinita, questo tipo di file viene salvato nella directory `conf`. Per interrompere la scrittura di questi file, impostare l'opzione su `false`.<br>In alternativa, è possibile modificare il percorso della directory in cui vengono salvati i file utilizzando `process.lastRunOutputDirectory`.<br>Valore di esempio: `true` |
| `process.encryptionKeyFile` | stringa (nome di file) | N/D | Nome del file contenente la chiave di crittografia. Vedere Crittografia dalla riga di comando a pagina 399.<br>Valore di esempio: `c:\dataloader\conf\my.key` |
| `process.initialLastRunDate` | data | N/D | Impostazione iniziale del parametro `process.lastRunDate` che può essere utilizzata in una stringa SQL e viene aggiornata automaticamente al termine dell'esecuzione di un |

| Nome parametro | Tipo di dati | Opzione equivalente della finestra di dialogo Impostazioni | Descrizione |
|---|---|---|---|
| | | | processo. Per una descrizione della sintassi del formato di data, vedere Formati di data a pagina 389.<br>Il formato deve essere `aaaa-MM-ggTHH:mm:ss.SSS+/-HHmm`. Ad esempio: 2006-04-13T13:50:32.423-0700 |
| `process.lastRunOutputDirectory` | stringa (directory) | N/D | Quando si esegue Data Loader nella modalità gruppi è possibile modificare il percorso in cui vengono scritti i file di output, ad esempio `sendAccountsFile_lastRun.properties`. Per impostazione predefinita, questo tipo di file viene salvato nella directory `\conf`. Per cambiare il percorso, modificare il valore dell'opzione specificando il percorso completo in cui si desidera scrivere i file di output.<br>In alternativa, è possibile impedire la scrittura dei file utilizzando `process.enableLastRunOutput`. |
| `process.loadRowToStartAt` | numero | `Start at row` | Se l'ultima operazione non è riuscita, è possibile utilizzare questa impostazione per ricominciare dal punto in cui l'ultima operazione riuscita era stata terminata.<br>Valore di esempio: `1008` |
| `process.mappingFile` | stringa (nome di file) | N/D | Nome del file di mappatura dei campi da utilizzare. Vedere Mappatura di colonne a pagina 416.<br>Valore di esempio: `c:\dataloader\conf\accountExtractMap.sdl` |
| `process.operation` | stringa | N/D | Operazione da eseguire. Vedere Operazioni dalla riga di comando di Data Loader a pagina 411.<br>Valore di esempio: `extract` |
| `process.statusOutputDirectory` | stringa (directory) | N/D | Directory nella quale vengono salvati i file di output "success" e "error". I nomi file vengono generati automaticamente per ciascuna operazione, se non diversamente specificato in `process-conf.xml`.<br>Valore di esempio: `c:\dataloader\status` |

| Nome parametro | Tipo di dati | Opzione equivalente della finestra di dialogo Impostazioni | Descrizione |
| --- | --- | --- | --- |
| process.outputError | stringa (nome di file) | N/D | Nome del file CSV in cui sono memorizzati i dati di errore dell'ultima operazione.<br>Valore di esempio: c:\dataloader\status\myProcessErrors.csv |
| process.outputSuccess | stringa (nome di file) | N/D | Nome del file CSV in cui sono memorizzati i dati di completamento dell'ultima operazione. Vedere anche process.enableExtractStatusOutput a pagina 403.<br>Valore di esempio: c:\dataloader\status\myProcessSuccesses.csv |
| process.useEuropeanDates | booleano | Use European date format | Selezionare questa opzione se si desidera utilizzare i formati data gg/MM/aaaa e gg/MM/aaaa HH:mm:ss.<br>Valore di esempio: true |
| sfdc.assignmentRule | stringa | Assignment rule | Specificare l'ID della regola di assegnazione da utilizzare per inserimenti, aggiornamenti e inserimenti con aggiornamento. Questa opzione è valida per gli inserimenti, gli aggiornamenti e gli inserimenti con aggiornamento di casi e lead. È valida inoltre per gli aggiornamenti degli account se l'organizzazione dispone di regole di assegnazione dei territori per gli account. La regola di assegnazione sovrascrive i valori Owner nel file CSV.<br>Valore di esempio: 03Mc00000026J7w |
| sfdc.bulkApiCheckStatusInterval | intero | N/D | Numero di millisecondi di attesa tra le singole verifiche per determinare il completamento dell'operazione di API in blocco asincrona e il numero di record elaborati. Vedere anche sfdc.useBulkApi. Si consiglia di specificare il valore 5000.<br>Valore di esempio: 5000 |
| sfdc.bulkApiSerialMode | booleano | Enable serial mode for Bulk API | Selezionare questa opzione per utilizzare l'elaborazione seriale anziché quella parallela per l'API in blocco. L'elaborazione in parallelo può causare conflitti per l'uso del database. Nei casi più gravi, il caricamento può non riuscire. L'utilizzo della modalità |

| Nome parametro | Tipo di dati | Opzione equivalente della finestra di dialogo Impostazioni | Descrizione |
|---|---|---|---|
| | | | seriale fa sì che i batch vengano elaborati uno alla volta. Tenere presente che l'uso di questa opzione può incrementare in modo considerevole il tempo di elaborazione di un carico. Vedere anche `sfdc.useBulkApi`.<br>Valore di esempio: `false` |
| `sfdc.bulkApiZipContent` | booleano | `Upload Bulk API Batch as Zip File` | Selezionare questa opzione per utilizzare l'API in blocco per il caricamento di file zip contenenti allegati binari, ad esempio record Allegato o Salesforce CRM Content. Vedere anche `sfdc.useBulkApi`.<br>Valore di esempio: `true` |
| `sfdc.connectionTimeoutSecs` | intero | N/D | Numero di secondi di attesa di una connessione durante le chiamate API.<br>Valore di esempio: `60` |
| `sfdc.debugMessages` | booleano | N/D | Se il valore è true, abilita il debug dei messaggi SOAP. Per impostazione predefinita, i messaggi vengono inviati a STDOUT, a meno che non venga specificato un percorso diverso in `sfdc.debugMessagesFile`.<br>Valore di esempio: `false` |
| `sfdc.debugMessagesFile` | stringa (nome di file) | N/D | Vedere `process.enableExtractStatusOutput` a pagina 403. Memorizza i messaggi SOAP inviati a o provenienti da Salesforce. I messaggi inviati o ricevuti vengono aggiunti alla fine del file. Poiché la dimensione del file è illimitata, verificare lo spazio su disco disponibile.<br>Valore di esempio: `\lexiloader\status\sfdcSoapTrace.log` |
| `sfdc.enableRetries` | booleano | N/D | Se il valore è true, abilita la ripetizione dei tentativi di connessione ai server di Salesforce. Vedere `sfdc.maxRetries` a pagina 408 e `sfdc.minRetrySleepSecs` a pagina 408.<br>Valore di esempio: `true` |

| Nome parametro | Tipo di dati | Opzione equivalente della finestra di dialogo Impostazioni | Descrizione |
|---|---|---|---|
| `sfdc.endpoint` | URL | `Server host` | Immettere l'URL del server Salesforce con cui si desidera comunicare. Ad esempio, se si stanno caricando dati in un Sandbox, l'URL in `https://test.salesforce.com`.<br>Valore di produzione di esempio: `https://login.salesforce.com/services/Soap/u/35.0` |
| `sfdc.entity` | stringa | N/D | Oggetto di Salesforce utilizzato nell'operazione.<br>Valore di esempio: `Lead` |
| `sfdc.externalIdField` | stringa | N/D | Utilizzato nelle operazioni di inserimento con aggiornamento; specifica il campo personalizzato con l'attributo "ID esterno" utilizzato come identificatore univoco per la corrispondenza dei dati.<br>Valore di esempio: `LegacySKU__c` |
| `sfdc.extractionRequestSize` | intero | `Query request size` | In un'unica operazione di esportazione o di query, i record vengono restituiti da Salesforce in incrementi di queste dimensioni. Il valore massimo è 2.000 record. Se si specifica un valore superiore, le prestazioni possono migliorare ma viene utilizzata più memoria sul client.<br>Valore di esempio: `500` |
| `sfdc.extractionSOQL` | stringa | N/D | Query SOQL per l'esportazione dei dati.<br>Valore di esempio: `SELECT Id, LastName, FirstName, Rating, AnnualRevenue, OwnerId FROM Lead` |
| `sfdc.insertNulls` | booleano | `Insert null values` | Selezionare questa opzione per inserire i valori mappati vuoti come valori `null` durante le operazioni sui dati. Tenere presente che, durante l'aggiornamento dei record, questa opzione trasmetterà a Data Loader l'istruzione di sovrascrivere i dati esistenti nei campi mappati.<br>Valore di esempio: `false` |
| `sfdc.loadBatchSize` | intero | `Batch size` | In un'unica operazione di inserimento, aggiornamento, inserimento con aggiornamento ed eliminazione, i movimenti di record da o a Salesforce vengono elaborati in incrementi di queste |

| Nome parametro | Tipo di dati | Opzione equivalente della finestra di dialogo Impostazioni | Descrizione |
|---|---|---|---|
| | | | dimensioni. Il valore massimo è 200. Si consiglia di utilizzare un valore compreso tra 50 e 100.<br>Valore di esempio: `100` |
| `sfdc.maxRetries` | intero | N/D | Numero massimo di tentativi di connessione a Salesforce. Vedere `sfdc.enableRetries` a pagina 406.<br>Valore di esempio: `3` |
| `sfdc.minRetrySleepSecs` | intero | N/D | Numero minimo di secondi di attesa tra i tentativi di connessione. Il tempo di attesa aumenta a ogni tentativo. Vedere `sfdc.enableRetries` a pagina 406.<br>Valore di esempio: `2` |
| `sfdc.noCompression` | booleano | `Compression` | L'opzione di compressione migliora le prestazioni di Data Loader ed è attivata per impostazione predefinita. Se è necessario eseguire il debug dei messaggi SOAP (Simple Object Access Protocol) sottostanti, è consigliabile disabilitare la compressione. Per disattivare la compressione, abilitare questa opzione.<br>Valore di esempio: `false` |
| `sfdc.password` | stringa crittografata | N/D | Password di Salesforce crittografata corrispondente al nome utente specificato in `sfdc.username`. Vedere anche Crittografia dalla riga di comando a pagina 399.<br>Valore di esempio: `4285b36161c65a22` |
| `sfdc.proxyHost` | URL | `Proxy host` | Il nome host del server proxy, quando applicabile.<br>Valore di esempio: `http://myproxy.internal.company.com` |
| `sfdc.proxyPassword` | stringa crittografata | `Proxy password` | Password crittografata corrispondente al nome utente proxy specificato in `sfdc.proxyUsername`. Vedere anche Crittografia dalla riga di comando a pagina 399.<br>Valore di esempio: `4285b36161c65a22` |

| Nome parametro | Tipo di dati | Opzione equivalente della finestra di dialogo Impostazioni | Descrizione |
|---|---|---|---|
| `sfdc.proxyPort` | intero | `Proxy port` | La porta del server proxy.<br>Valore di esempio: `8000` |
| `sfdc.proxyUsername` | stringa | `Proxy username` | Il nome utente per l'autenticazione del server proxy.<br>Valore di esempio: `jane.doe` |
| `sfdc.resetUrlOnLogin` | booleano | `Reset URL on Login` | Per impostazione predefinita, Salesforce reimposta l'URL dopo che si è effettuato l'accesso a quello specificato in `sfdc.endpoint`. Per disattivare questa reimpostazione automatica, disabilitare l'opzione impostandola su `false`.<br>Valori validi: `true` (predefinito), `false` |
| `sfdc.timeoutSecs` | intero | `Timeout` | Indica per quanti secondi Data Loader attende una risposta dal server prima di segnalare un errore per la richiesta.<br>Valore di esempio: `540` |
| `sfdc.timezone` | stringa | `Fuso orario` | Se il valore di una data non include il fuso orario, viene utilizzato questo valore.<br>• Se non è specificato alcun valore, viene utilizzato il fuso orario del computer in cui è installato Data Loader.<br>• Se è specificato un valore errato, viene utilizzato il fuso orario GMT e l'errore viene segnalato nel registro di Data Loader.<br>Sono validi tutti gli indicatori di fuso orario che possono essere passati al metodo `getTimeZone(java.lang.String)` Java. Il valore può essere costituito da un nome esteso, ad esempio `America/Los_Angeles`, o da un ID personalizzato, ad esempio `GMT-8:00`.<br>È possibile recuperare il valore predefinito eseguendo il metodo `TimeZone.getDefault()` in Java. Questo valore rappresenta il fuso orario del computer su cui è installato Data Loader. |
| `sfdc.truncateFields` | booleano | `Allow field truncation` | Selezionare questa opzione per fare in modo che i dati vengano troncati nei seguenti tipi di campi durante il caricamento dei dati in Salesforce: Email, |

| Nome parametro | Tipo di dati | Opzione equivalente della finestra di dialogo Impostazioni | Descrizione |
|---|---|---|---|
| | | | Elenco di selezione a selezione multipla, Telefono, Elenco di selezione, Testo e Testo (crittografato).<br>In Data Loader versione 14.0 e precedenti, i valori di questi tipi di campi vengono troncati se troppo lunghi. In Data Loader versione 15.0 e successive, l'operazione di caricamento non viene eseguita se un valore specificato è troppo lungo.<br>La selezione di questa opzione consente di richiedere l'utilizzo del comportamento precedente, vale a dire del troncamento, invece del nuovo comportamento previsto nelle versioni 15.0 e successive di Data Loader. Questa opzione è selezionata per impostazione predefinita e non ha alcun effetto nelle versioni 14.0 e precedenti.<br>Questa opzione non è disponibile se è selezionata l'opzione `Use Bulk API`. In tal caso, l'operazione di caricamento per la riga non riesce se è stato specificato un valore troppo grande per il campo.<br>Valore di esempio: `true` |
| `sfdc.useBulkApi` | booleano | `Use Bulk API` | Selezionare questa opzione per utilizzare l'API in blocco per inserire, aggiornare, inserire con aggiornamento, eliminare ed eliminare definitivamente i record. L'API in blocco è ottimizzata in modo da caricare o eliminare un numero elevato di record in modo asincrono ed è più rapida dell'API basata su SOAP predefinita grazie all'elaborazione parallela e al minor numero di viaggi di andata e ritorno nella rete. Vedere anche `sfdc.bulkApiSerialMode`.<br>Valore di esempio: `true` |
| `sfdc.username` | stringa | N/D | Nome utente di Salesforce. Vedere `sfdc.password`.<br>Valore di esempio: `jdoe@mycompany.com` |

## Operazioni dalla riga di comando di Data Loader

Nota: l'interfaccia della riga di comando di Data Loader è supportata solo per Windows.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Quando si esegue Data Loader nella modalità a gruppi dalla riga di comando, sono supportate diverse operazioni. Un'operazione rappresenta un flusso di dati tra Salesforce e una fonte di dati esterna, ad esempio un file CSV o un database. Fare riferimento al seguente elenco di nomi di operazioni e descrizioni.

**Extract**
: Viene utilizzata una Salesforce Object Query Language per esportare un set di record da Salesforce e i dati esportati vengono scritti in una fonte di dati. I record eliminati in modo non definitivo non sono inclusi.

**Extract All**
: Viene utilizzata una Salesforce Object Query Language per esportare un set di record da Salesforce, inclusi i record esistenti e quelli eliminati in modo non definitivo, e i dati esportati vengono scritti in una fonte di dati.

**Insert**
: I dati di una fonte di dati vengono caricati in Salesforce come nuovi record.

**Update**
: I dati di una fonte di dati vengono caricati in Salesforce dove vengono aggiornati i record esistenti con campi ID corrispondenti.

**Upsert**
: I dati di una fonte di dati vengono caricati in Salesforce dove vengono aggiornati i record esistenti con campo ID esterno personalizzato corrispondente; i record senza corrispondenza vengono inseriti come nuovi record.

**Delete**
: I dati di una fonte di dati vengono caricati in Salesforce dove i record esistenti con campi ID corrispondenti vengono eliminati.

**Hard Delete**
: I dati di una fonte di dati vengono caricati in Salesforce, dove i record esistenti con campi ID corrispondenti vengono eliminati definitivamente senza essere prima spostati nel Cestino.

## Configurazione dell'accesso al database

Nota: l'interfaccia della riga di comando di Data Loader è supportata solo per Windows.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Quando Data Loader viene eseguito in modalità a gruppi dalla riga di comando, utilizzare `\samples\conf\database-conf.xml` per configurare gli oggetti di accesso al database utilizzati per estrarre i dati direttamente da un database.

### Bean DatabaseConfig

L'oggetto di configurazione del database di livello superiore è il bean `DatabaseConfig` con le seguenti proprietà:

**sqlConfig**
: Bean di configurazione SQL per l'oggetto di accesso ai dati che interagisce con un database.

**dataSource**
: Bean con funzione di driver di database e autenticatore. È necessario che il bean faccia riferimento a un'implementazione di `javax.sql.DataSource` quale `org.apache.commons.dbcp.BasicDataSource`.

Il codice riportato di seguito è un esempio di bean DatabaseConfig:

```
<bean id="AccountInsert"
    class="com.salesforce.dataloader.dao.database.DatabaseConfig"
    singleton="true">
    <property name="sqlConfig" ref="accountInsertSql"/>
</bean>
```

## DataSource

Il bean `DataSource` consente di impostare le informazioni fisiche necessarie per le connessioni al database. Contiene le seguenti proprietà:

**driverClassName**
Nome completo dell'implementazione di un driver JDBC.

**url**
Stringa per la connessione fisica al database.

**username**
Nome utente per l'accesso al database.

**password**
Password per l'accesso al database.

A seconda dell'implementazione, potrebbe essere necessario immettere ulteriori informazioni. Utilizzare ad esempio `org.apache.commons.dbcp.BasicDataSource` quando le connessioni al database sono inserite in un pool.

Il codice riportato di seguito è un esempio di bean DataSource:

```
<bean id="oracleRepDataSource"
    class="org.apache.commons.dbcp.BasicDataSource"
    destroy-method="close">
    <property name="driverClassName" value="oracle.jdbc.driver.OracleDriver"/>
    <property name="url" value="jdbc:oracle:thin:@myserver.salesforce.com:1521:TEST"/>
    <property name="username" value="test"/>
    <property name="password" value="test"/>
</bean>
```

Le versioni di Data Loader dall'API versione 25.0 in poi non dispongono di un driver JDBC Oracle. Utilizzare Data Loader per la connessione a una fonte di dati Oracle senza installare un driver JDBC causerà un errore di caricamento della classe di driver JDBC. Per aggiungere il driver JDBC Oracle a Data Loader:

- Scaricare il driver JDBC più recente da `http://www.oracle.com/technetwork/database/features/jdbc/index-091264.html`.
- Copiare il file JDBC .jar in *`cartella di installazione di data loader`*`/java/bin`.

VEDERE ANCHE:

Framework Spring
Oggetti di accesso ai dati
Configurazione SQL

## Framework Spring

Nota: l'interfaccia della riga di comando di Data Loader è supportata solo per Windows.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

I file di configurazione di Data Loader sono basati sul framework Spring, un framework di applicazione Java/J2EE, a stack pieno open source.

Il framework Spring consente di utilizzare i file XML per la configurazione dei bean. Ogni bean rappresenta un'istanza di un oggetto; i parametri corrispondono ai metodi di impostazione di ogni oggetto. Un bean tipico presenta i seguenti attributi:

**id**
: Identifica in modo univoco il bean in `XmlBeanFactory`, la classe che ottiene gli oggetti da un file di configurazione XML.

**class**
: Specifica la classe di implementazione dell'istanza del bean.

Per ulteriori informazioni sul framework Spring, vedere la documentazione ufficiale e i forum di assistenza. Tenere presente che Salesforce non può garantire la disponibilità o l'accuratezza dei siti Web esterni.

VEDERE ANCHE:

Configurazione dell'accesso al database

## Oggetti di accesso ai dati

Nota: l'interfaccia della riga di comando di Data Loader è supportata solo per Windows.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Quando si esegue Data Loader nella modalità a gruppi dalla riga di comando, sono supportati diversi oggetti di accesso ai dati. Un oggetto di accesso ai dati consente di accedere a una fonte di dati esterna a Salesforce. L'oggetto può implementare un'interfaccia di lettura (`DataReader`), un'interfaccia di scrittura (`DataWriter`) o entrambe. Fare riferimento al seguente elenco di nomi e descrizioni di oggetti.

**csvRead**
: Consente la lettura di un file delimitato da virgole o tabulazioni. Nella parte superiore del file deve essere presente una riga di intestazione che descrive ciascuna colonna.

**csvWrite**
: Consente la scrittura in un file delimitato da virgole. Nella parte superiore del file viene aggiunta una riga di intestazione in base all'elenco di colonne fornito dal chiamante.

**databaseRead**
: Consente la lettura di un database. Utilizzare `database-conf.xml` per configurare l'accesso al database.

**databaseWrite**
: Consente la scrittura in un database. Utilizzare `database-conf.xml` per configurare l'accesso al database.

VEDERE ANCHE:

Configurazione dell'accesso al database

## Configurazione SQL

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Nota: l'interfaccia della riga di comando di Data Loader è supportata solo per Windows.

Quando Data Loader viene eseguito in modalità a gruppi dalla riga di comando, la classe `SqlConfig` contiene parametri di configurazione per l'accesso a specifici dati nel database. Come illustrato negli esempi di codice riportati di seguito, sebbene diversi, le query e gli inserimenti sono molto simili. Il bean deve essere di tipo `com.salesforce.dataloader.dao.database.SqlConfig` e avere le seguenti proprietà:

**`sqlString`**
: Codice SQL che deve essere utilizzato dall'oggetto di accesso ai dati.

Il codice SQL può contenere parametri di sostituzione che rendono la stringa dipendente da variabili di configurazione e operazione. I parametri di sostituzione devono essere delimitati su entrambi i lati dai caratteri "@". Ad esempio, `@process.lastRunDate@`.

**`sqlParams`**
: Proprietà di tipo `map` contenente le descrizioni dei parametri di sostituzione specificati in `sqlString`. Ogni voce rappresenta un parametro di sostituzione: la chiave corrisponde al nome del parametro di sostituzione, mentre il valore corrisponde al tipo Java da utilizzare quando il parametro viene impostato sull'istruzione SQL. Tenere presente che a volte sono necessari tipi "java.sql" come `java.sql.Date` anziché `java.util.Date`. Per ulteriori informazioni, vedere la documentazione ufficiale dell'API JDBC.

**`columnNames`**
: Utilizzata quando le query (istruzioni `SELECT`) restituiscono un `ResultSet` JDBC. Contiene i nomi di colonna dei dati generati eseguendo l'istruzione SQL. I nomi di colonna vengono utilizzati per accedere e restituire l'output al chiamante dell'interfaccia `DataReader`.

### Esempio di bean di query SQL

```
<bean id="accountMasterSql"
    class="com.salesforce.dataloader.dao.database.SqlConfig"
    singleton="true">
    <property name="sqlString"/>
        <value>
            SELECT distinct
                '012x00000000Ij7' recordTypeId,
                accounts.account_number,
                org.organization_name,
                concat (concat(parties.address1, ' '), parties.address2) billing_address,

                locs.city,
                locs.postal_code,
                locs.state,
                locs.country,
                parties.sic_code
            from
                ar.hz_cust_accounts accounts,
                ar.hz_organization_profiles org,
                ar.hz_parties parties,
                ar.hz_party_sites party_sites,
                ar.hz_locations locs
            where
```

```
                accounts.PARTY_ID = org.PARTY_ID
                and parties.PARTY_ID = accounts.PARTY_ID
                and party_sites.PARTY_ID = accounts.PARTY_ID
                and locs.LOCATION_ID = party_sites.LOCATION_ID
                and (locs.last_update_date > @process.lastRunDate@ OR
accounts.last_update_date > @process.lastRunDate@
        </value>
    </property>
    <property name="columNames">
        <list>
            <value>recordTypeId</value>
            <value>account_number</value>
            <value>organization_name</value>
            <value>billing_address</value>
            <value>city</value>
            <value>postal_code</value>
            <value>state</value>
            <value>country</value>
            <value>sic_code</value>
        </list>
    </property>
    <property name="sqlParams">
        <map>
            <entry key="process.lastRunDate" value="java.sql.Date"/>
        </map>
    </property>
</bean>
```

Esempio di bean di inserimento SQL

```
<bean id="partiesInsertSql"
    class="com.salesforce.dataloader.dao.database.SqlConfig"
    singleton="true">
    <property name="sqlString"/>
        <value>
            INSERT INTO REP.INT_PARTIES (
            BILLING_ADDRESS, SIC_CODE)
            VALUES (@billing_address@, @sic_code@)
        </value>
    </property>
    <property name="sqlParams"/>
        <map>
            <entry key="billing_address" value="java.lang.String"/>
            <entry key="sic_code" value="java.lang.String"/>
        </map>
    </property>
</bean>
```

VEDERE ANCHE:

Configurazione dell'accesso al database

## Mappatura di colonne

Nota: l'interfaccia della riga di comando di Data Loader è supportata solo per Windows.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Quando si esegue Data Loader nella modalità a gruppi dalla riga di comando, è necessario creare un file delle proprietà per la mappatura dei valori tra Salesforce e gli oggetti di accesso ai dati.

1. Creare un nuovo file di mappatura con estensione `.sdl`.
2. Utilizzare la seguente sintassi:
   - In ciascuna riga, associare ogni fonte di dati alla destinazione.
   - In un file di importazione, specificare la fonte di dati a sinistra, un segno di uguale (=) come separatore e la destinazione a destra. In un file di esportazione, specificare la destinazione a sinistra, un segno di uguale (=) come separatore e la fonte di dati a destra.
   - Le fonti di dati possono essere costituite da nomi di colonna o da costanti. Specificare le costanti tra virgolette doppie, ad esempio "costantediesempio". I valori tra virgolette vengono considerati come nomi di colonna.
   - Le destinazioni devono essere costituite da nomi di colonna.
   - È possibile mappare le costanti specificandole tra virgolette doppie, ad esempio:

     ```
     "Canada"=BillingCountry
     ```

3. Nel file di configurazione, utilizzare il parametro `process.mappingFile` per specificare il nome del file di mappatura.

Nota: Se il nome del campo contiene uno spazio, è necessario utilizzare la sequenza escape sullo spazio facendolo precedere da una barra rovesciata (\). Ad esempio:

```
Account\ Name=Name
```

### Esempio di mappatura di colonne per l'inserimento di dati

I campi Salesforce sono specificati a destra.

```
SLA__C=SLA__c
BILLINGCITY=BillingCity
SYSTEMMODSTAMP=
OWNERID=OwnerId
CUSTOMERPRIORITY__C=CustomerPriority__c
ANNUALREVENUE=AnnualRevenue
DESCRIPTION=Description
BILLINGSTREET=BillingStreet
SHIPPINGSTATE=ShippingState
```

### Esempio di mappatura di colonne per l'esportazione di dati

I campi Salesforce sono specificati a sinistra.

```
Id=account_number
Name=name
Phone=phone
```

### Mappatura di colonne per i valori delle costanti

Data Loader consente di assegnare costanti ai campi quando si inseriscono, si aggiornano e si esportano i dati. Se un campo deve contenere lo stesso valore per ogni record, è necessario specificare la costante nel file di mappatura `.sdl` anziché specificare il campo e il valore nel file CSV o nella query di esportazione.

La costante deve essere racchiusa tra virgolette doppie. Ad esempio, se si importano dati, la sintassi è `"constantvalue"=field1`.

Se più campi devono contenere lo stesso valore, è necessario specificare la costante e il nome del campo separandoli con virgole. Ad esempio, se si importano dati, la sintassi sarebbe `"constantvalue"=field1, field2`.

Di seguito è riportato un esempio di file `.sdl` per l'inserimento di dati. I campi Salesforce sono specificati a destra. Le prime due righe mappano una fonte di dati a un campo di destinazione e le ultime tre righe mappano una costante a un campo di destinazione.

```
Name=Name
NumEmployees=NumberOfEmployees
"Aerospace"=Industry
"California"=BillingState, ShippingState
"New"=Customer_Type__c
```

Una costante deve contenere almeno un carattere alfanumerico.

Nota: Se si specifica un valore costante contenente degli spazi, è necessario utilizzare la sequenza escape su tali spazi facendo precedere ognuno da una barra rovesciata (\). Ad esempio:

```
"Food\ &\ Beverage"=Industry
```

## Esecuzione di processi batch singoli

Nota: l'interfaccia della riga di comando di Data Loader è supportata solo per Windows.

Per avviare un singolo processo batch utilizzare `\bin\process.bat` che richiede i seguenti parametri:

**Una directory di configurazione**

Il valore predefinito è `\conf`.

Per utilizzare una directory diversa, creare una nuova directory e aggiungere i seguenti file alla directory:

- Se il processo non è interattivo, copiare `process-conf.xml` da `\samples\conf`.
- Se il processo richiede la connettività database, copiare `database-conf.xml` da `\samples\conf`.
- Copiare `config.properties` da `\conf`.

**Un nome di processo**

Il nome del bean ProcessRunner da `\samples\conf\process-conf.xml`.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

### Esempio di processo

```
process ../conf accountMasterProcess
```

Nota: È possibile configurare programmi di avvio dei processi esterni, ad esempio Pianificazione guidata operazioni di Microsoft Windows XP, per l'esecuzione pianificata dei processi.

# Avvio rapido da riga di comando (solo Windows)

## Introduzione a Data Loader

Nota: l'interfaccia della riga di comando di Data Loader è supportata solo per Windows.

Oltre a utilizzare Data Loader in modo interattivo per importare ed esportare i dati, è possibile eseguirlo dalla riga di comando. È possibile utilizzare i comandi per automatizzare l'importazione e l'esportazione dei dati.

Questo programma di avvio rapido mostra in che modo utilizzare la funzionalità della riga di comando di Data Loader per importare i dati. Eseguire le seguenti operazioni.

- Fase 1: creare la chiave di crittografia
- Fase 2: creare la password crittografata per il nome utente di accesso
- Fase 3: creare il file di mappatura dei campi
- Fase 4: creare un file `process-conf.xml` contenente le impostazioni di configurazione dell'importazione
- Fase 5: eseguire il processo e importare i dati

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

## Prerequisiti

Nota: l'interfaccia della riga di comando di Data Loader è supportata solo per Windows.

Per eseguire questo avvio rapido, è necessario disporre di quanto segue:

- Data Loader installato sul computer che esegue il processo della riga di comando.
- Java Runtime Environment (JRE) installato sul computer che esegue il processo della riga di comando.
- Avere dimestichezza con l'importazione e l'esportazione dei dati utilizzando Data Loader in modo interattivo mediante l'interfaccia utente. Questo facilita la comprensione della funzionalità della riga di comando.

Suggerimento: Quando si installa Data Loader, nella directory samples vengono installati i file di esempio. Questa directory si trova sotto la directory dei programmi, ad esempio `C:\Programmi (x86)\salesforce.com\Apex Data Loader 22.0\samples\`. Gli esempi dei file utilizzati in questo avvio rapido si trovano nella directory `\samples\conf`.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

## Fase 1: creare la chiave di crittografia

Nota: l'interfaccia della riga di comando di Data Loader è supportata solo per Windows.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Quando si utilizza Data Loader dalla riga di comando, non vi è alcuna interfaccia utente. Pertanto, è necessario fornire le informazioni che normalmente verrebbero immesse nell'interfaccia utente utilizzando un file di testo denominato `process-conf.xml`. Ad esempio, aggiungere il nome utente e la password utilizzati da Data Loader per accedere a Salesforce. La password deve essere crittografata prima di essere aggiunta al file `process-conf.xml` e la creazione della chiave rappresenta la prima fase di quel processo.

1. Aprire una finestra prompt dei comandi facendo clic su **Start** > **Tutti i programmi** > **Accessori** > **Prompt dei comandi**. In alternativa, fare clic su **Start** > **Esegui**, immettere *cmd* nel campo **Apri** e fare clic su **OK**.
2. Nella finestra dei comandi, immettere *cd* per andare alla directory principale dell'unità in cui Data Loader è installato.
3. Andare alla directory `\bin` di Data Loader immettendo questo comando. Assicurarsi di sostituire il percorso del file con il percorso del proprio sistema.

   ```
   cd C:\Programmi (x86)\salesforce.com\Apex Data Loader 22.0\bin
   ```

4. Creare una chiave di crittografia immettendo il seguente comando. Sostituire <seedtext> con qualsiasi stringa.

   ```
   encrypt.bat —g <seedtext>
   ```

   Nota: per visualizzare un elenco delle opzioni della riga di comando per `encrypt.bat`, digitare *encrypt.bat* sulla riga di comando.

5. Copiare la chiave generata dalla finestra dei comandi in un file di testo denominato `key.txt` e prendere nota del percorso del file. In questo esempio, la chiave generata è `e8a68b73992a7a54`.

   Nota: L'abilitazione della modalità di modifica rapida in una finestra dei comandi può facilitare la copia dei dati da e nella finestra. Per abilitare la modalità di modifica rapida, fare clic con il pulsante destro del mouse sul margine superiore della finestra e selezionare **Proprietà**. Nella scheda **Opzioni**, selezionare **Modalità Modifica rapida**.

L'utility di crittografia viene utilizzata per crittografare le password, ma i dati trasmessi con Data Loader non vengono crittografati.

VEDERE ANCHE:

Fase 2: creare la password crittografata

## Fase 2: creare la password crittografata

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Nota: l'interfaccia della riga di comando di Data Loader è supportata solo per Windows.

In questa fase, viene creata la password crittografata utilizzando la chiave generata nella fase precedente.

1. Nella stessa finestra del prompt dei comandi, immettere il comando seguente. Sostituire <password> con la password utilizzata da Data Loader per accedere a Salesforce. Sostituire <filepath> con il percorso del file `key.txt` creato nella fase precedente.

   ```
   encrypt.bat -e <password> "<filepath>\key.txt"
   ```

2. Copiare la password crittografata generata dal comando. Questo valore verrà utilizzato in una fase successiva.

VEDERE ANCHE:

Fase 3: creare il file di mappatura dei campi

## Fase 3: creare il file di mappatura dei campi

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Nota: l'interfaccia della riga di comando di Data Loader è supportata solo per Windows.

Il file di mappatura dei campi consente di associare le sorgenti di dati alle destinazioni. Si tratta di un file di testo, tipicamente con estensione `.sdl`.

1. Copiare quanto segue in un file di testo e salvarlo con il nome `accountInsertMap.sdl`. Poiché si tratta di un inserimento di dati, la sorgente dei dati si trova a sinistra del segno di uguale e il campo di destinazione si trova a destra.

```
#Mapping values
#Thu May 26 16:19:33 GMT 2011
Name=Name
NumberOfEmployees=NumberOfEmployees
Industry=Industry
```

Suggerimento: nel caso di mappature complesse, è possibile utilizzare l'interfaccia utente di Data Loader per eseguire la mappatura dei campi sorgente e destinazione e, in seguito, salvare le mappature in un file `.sdl`. A questo scopo, nella finestra di dialogo Mapping, fare clic su **Save Mapping**.

VEDERE ANCHE:

Fase 4: creare il file di configurazione

## Fase 4: creare il file di configurazione

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

**Nota:** l'interfaccia della riga di comando di Data Loader è supportata solo per Windows.

Il file `process-conf.xml` contiene le informazioni necessarie a Data Loader per elaborare i dati. Ogni `<bean>` nel file `process-conf.xml` fa riferimento a un unico processo, quale un inserimento, un inserimento con aggiornamento, un'esportazione, e così via. Pertanto, questo file può contenere più processi. In questa fase, viene modificato il file in modo da inserire gli account in Salesforce.

1. Creare una copia del file `process-conf.xml` dalla directory `\samples\conf`. Assicurarsi di tenere una copia dell'originale, in quanto contiene esempi di altri tipi di elaborazioni Data Loader, quali gli inserimenti con aggiornamenti e le esportazioni.
2. Aprire il file in un editor di testo e sostituire il contenuto con il seguente XML:

```
<!DOCTYPE beans PUBLIC "-//SPRING//DTD BEAN//EN"
"http://www.springframework.org/dtd/spring-beans.dtd">
<beans>
    <bean id="accountInsert"
        class="com.salesforce.dataloader.process.ProcessRunner"
        singleton="false">
        <description>accountInsert job gets the account record from the CSV file
            and inserts it into Salesforce.</description>
        <property name="name" value="accountInsert"/>
        <property name="configOverrideMap">
            <map>
                <entry key="sfdc.debugMessages" value="true"/>
                <entry key="sfdc.debugMessagesFile"
                    value="C:\DLTest\Log\accountInsertSoapTrace.log"/>
                <entry key="sfdc.endpoint" value="https://servername.salesforce.com"/>
                <entry key="sfdc.username" value="admin@Org.org"/>
                <!--Password below has been encrypted using key file,
                    therefore, it will not work without the key setting:
                    process.encryptionKeyFile.
                    The password is not a valid encrypted value,
                    please generate the real value using the encrypt.bat utility -->
                <entry key="sfdc.password" value="e8a68b73992a7a54"/>
                <entry key="process.encryptionKeyFile"
                    value="C:\DLTest\Command Line\Config\key.txt"/>
                <entry key="sfdc.timeoutSecs" value="600"/>
                <entry key="sfdc.loadBatchSize" value="200"/>
                <entry key="sfdc.entity" value="Account"/>
                <entry key="process.operation" value="insert"/>
                <entry key="process.mappingFile"
                    value="C:\DLTest\Command Line\Config\accountInsertMap.sdl"/>
                <entry key="dataAccess.name"
                    value="C:\DLTest\In\insertAccounts.csv"/>
                <entry key="process.outputSuccess"
                    value="c:\DLTest\Log\accountInsert_success.csv"/>
                <entry key="process.outputError"
                    value="c:\DLTest\Log\accountInsert_error.csv"/>
                <entry key="dataAccess.type" value="csvRead"/>
                <entry key="process.initialLastRunDate"
                    value="2005-12-01T00:00:00.000-0800"/>
```

```
            </map>
        </property>
    </bean>
</beans>
```

3. Modificare i seguenti parametri nel file `process-conf.xml`. Per maggiori informazioni sui parametri di configurazione dei processi, vedere Parametri di configurazione dei processi Data Loader a pagina 402.
   - `sfdc.endpoint`: immettere l'URL dell'istanza Salesforce dell'organizzazione; ad esempio, `https://na1.salesforce.com`.
   - `sfdc.username`: immettere il nome utente che Data Loader utilizza per l'accesso.
   - `sfdc.password`: immettere il valore della password crittografata creato nella fase 2.
   - `process.mappingFile`: immettere il percorso e il nome file del file di mappatura.
   - `dataAccess.Name`: immettere il percorso e il nome del file di dati contenente gli account da importare.
   - `sfdc.debugMessages`: impostato su `true` per la risoluzione dei problemi. Impostare su `false` dopo che è stata avviata l'importazione.
   - `sfdc.debugMessagesFile`: immettere il percorso e il nome del file di registro della riga di comando.
   - `process.outputSuccess`: immettere il percorso e il nome del file di registro "success".
   - `process.outputError`: immettere il percorso e il nome del file di registro "error".

   Avvertenza: fare attenzione quando si utilizzano editor XML diversi per modificare il file `process-conf.xml`. Alcuni editor aggiungono tag XML all'inizio e alla fine del file, causando la non riuscita dell'importazione.

VEDERE ANCHE:

Fase 5: importare i dati

## Fase 5: importare i dati

| AUTORIZZAZIONI UTENTE | |
|---|---|
| Per inserire record: | "Crea" per il record |
| Per aggiornare i record: | "Modifica" per il record |
| Per aggiornare e inserire record: | "Crea" o "Modifica" per il record |
| Per eliminare i record: | "Elimina" per il record |
| Per eliminare definitivamente i record: | "Elimina" per il record |

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Nota: l'interfaccia della riga di comando di Data Loader è supportata solo per Windows.

Dopo avere completato tutte le fasi di preparazione, è possibile eseguire Data Loader dalla riga di comando e inserire i nuovi account.

1. Copiare i seguenti dati in un file denominato `accountInsert.csv`. Questi sono i dati degli account che vengono importati nell'organizzazione.

```
Name,Industry,NumberOfEmployees
Dickenson plc,Consulting,120
```

```
GenePoint,Biotechnology,265
Express Logistics and Transport,Transportation,12300
Grand Hotels & Resorts Ltd,Hospitality,5600
```

2. Nella finestra del prompt dei comandi, immettere il comando seguente:

   ```
   process.bat "<file path to process-conf.xml>" <process name>
   ```

   - Sostituire <file path to process-conf.xml> con il percorso della directory contenente `process-conf.xml`.
   - Sostituire <process name> con il processo specificato in `process-conf.xml`.

   Il comando dovrebbe avere l'aspetto seguente:

   ```
   process.bat "C:\DLTest\Command Line\Config" accountInsert
   ```

   Dopo l'esecuzione del processo, la finestra del prompt dei comandi visualizza i messaggi di riuscita e di errore. Inoltre, è possibile controllare i file di registro: `insertAccounts_success.csv` e `insertAccounts_error.csv`. Al termine dell'esecuzione corretta del processo, il file `insertAccounts_success.csv` contiene i record importati, con un'indicazione di ID e stato per ogni record. Per ulteriori informazioni sui file di stato, vedere Revisione dei file di output di Data Loader a pagina 397.

## Licenze di terze parti di Data Loader

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Le seguenti licenze di terze parti sono incluse con l'installazione di Data Loader:

| Tecnologia | Versione | Licenza |
|---|---|---|
| Apache Jakarta Commons BeanUtils | 1.6 | http://www.apache.org/licenses/LICENSE-2.0 |
| Apache Commons Collections | 3.1 | http://www.apache.org/licenses/LICENSE-2.0 |
| Apache Commons Database Connection Pooling (DBCP) | 1.2.1 | http://www.apache.org/licenses/LICENSE-2.0 |
| Apache Commons Logging | 1.0.3 | http://www.apache.org/licenses/LICENSE-1.1 |
| Apache Commons Object Pooling Library | 1.2 | http://www.apache.org/licenses/LICENSE-2.0 |
| Apache Log4j | 1.2.8 | http://www.apache.org/licenses/LICENSE-2.0 |
| Eclipse SWT | 3.452 | http://www.eclipse.org/legal/epl-v10.html |
| OpenSymphony Quartz Enterprise Job Scheduler | 1.5.1 | http://www.opensymphony.com/quartz/license.action |
| Rhino JavaScript for Java | 1.6R2 | http://www.mozilla.org/MPL/MPL-1.1.txt |
| Framework Spring | 1.2.6 | http://www.apache.org/licenses/LICENSE-2.0.txt |

Nota: Salesforce non è responsabile della disponibilità o dei contenuti dei siti Web di terze parti.

# Domande frequenti sull'importazione

## Domande generali sulle importazioni

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni.



VEDERE ANCHE:


Importazione di account personali

Importazione di membri della campagna


### Posso eseguire un caricamento globale di dati in Salesforce?

Le versioni Group Edition, Professional Edition, Performance Edition, Unlimited Edition, Enterprise Edition e Developer Edition dispongono di una procedura guidata di importazione dei dati per account, referenti, lead e oggetti personalizzati che consente di effettuare un'importazione globale dei dati. Per accedervi, da Imposta, fare clic su **Gestione dati**. Inoltre, le versioni Performance Edition, Unlimited Edition, Enterprise Edition e Developer Edition dispongono dell'accesso API per l'utilizzo di strumenti di caricamento globale nei database come Data Loader.

## È necessario sincronizzare Outlook o utilizzare le importazioni guidate per caricare i dati in Salesforce?

Utilizzare le seguenti informazioni per determinare in che modo caricare i dati nella propria organizzazione Salesforce.

- Per caricare account e referenti contemporaneamente per più utenti, utilizzare l'importazione guidata dati e selezionare **Account e referenti**.
- Per caricare i referenti da qualsiasi applicazione che non sia Microsoft Outlook, utilizzare l'importazione guidata dati e selezionare **Account e referenti**.
- Per tenere aggiornati i propri referenti, account ed eventi di calendario di Outlook con Salesforce, è consigliabile utilizzare Exchange Sync o Salesforce per Outlook per la prima sincronizzazione dei dati e per tutti i successivi aggiornamenti.
- Per caricare oggetti, soluzioni e lead personalizzati, utilizzare l'importazione guidata dati e selezionare l'oggetto appropriato per importare tali tipi di record in Salesforce. Non è possibile sincronizzare tali record utilizzando Exchange Sync o Salesforce per Outlook.
- Per caricare account aziendali e referenti contemporaneamente per più utenti, utilizzare l'importazione guidata dati e selezionare **Account e referenti**.
- Per caricare gli account personali, utilizzare l'importazione guidata degli account personali.

Nota: Quando si importano account personali, vengono applicate le seguenti limitazioni.

- L'importazione guidata dati unificata non supporta gli account personali.
- Non è possibile caricare gli account personali utilizzando Salesforce per Outlook.
- I referenti di Outlook possono essere sincronizzati con gli account personali in Salesforce solo se gli account personali esistono già. La sincronizzazione non converte i referenti di Outlook in account personali in Salesforce.

Per ulteriori informazioni sull'importazione degli account personali, vedere Importa account personali a pagina 373.

## Quali utenti dell'organizzazione possono utilizzare le importazioni guidate?

Tutti gli utenti dell'organizzazione possono utilizzare la procedura guidata Importa referenti personali. Nelle organizzazioni che utilizzano le versioni Enterprise Edition, Unlimited Edition, Performance Edition o Developer Edition con gli account personali abilitati, tutti gli utenti possono utilizzare la procedura guidata Importa account personali.

L'importazione guidata dei dati per account, referenti, lead, soluzioni o oggetti personalizzati a livello di organizzazione per più utenti contemporaneamente può essere utilizzata solo da un amministratore. Nella versione Personal Edition la procedura Importazione guidata dati non è disponibile. Nella versione Contact Manager Edition, lead e soluzioni non sono disponibili per l'importazione guidata dei dati. Nella versione Group Edition le soluzioni non sono disponibili per la procedura Importazione guidata dati.

Importante: Salesforce ha sostituito le singole procedure di importazione guidata per account, referenti e altri oggetti con una procedura unificata di Importazione guidata dati (le singole procedure di importazione guidata si aprono in piccole finestre popup, mentre l'importazione unificata si apre in un browser di dimensioni normali con dataimporter.app alla fine dell'URL). Per iniziare a utilizzare la procedura unificata, da Imposta, immettere *`Importazione guidata dati`* nella casella `Ricerca veloce`, quindi selezionare **Importazione guidata dati**. (le opzioni visualizzate dipendono dalle autorizzazioni di cui si dispone).

## Quali autorizzazioni occorrono per importare record?

### Data Loader

Per importare record con Data Loader è necessario disporre dell'autorizzazione "Crea" sul record da importare.

### Importazione guidata dei record di cui si è titolari

| Record da importare | Autorizzazione necessaria |
|---|---|
| Referenti personali | "Importa referenti personali" |
| Account personali | "Crea" per gli account<br>E<br>"Lettura" per i referenti<br>E<br>"Importa referenti personali"<br>E<br>Almeno un tipo di record account personale disponibile nel proprio profilo o negli insiemi di autorizzazioni |

### Importazione guidata dei record di cui non si è titolari

| Record da importare | Autorizzazione necessaria |
|---|---|
| Referenti e account dell'organizzazione | Amministratori<br>Gli utenti che dispongono dell'autorizzazione "Modifica tutti i dati" |
| Account personali dell'organizzazione | Tutti gli utenti che dispongono dell'autorizzazione "Modifica tutti i dati" |
| Lead dell'organizzazione | "Lettura", "Crea" e "Modifica" per i lead<br>E<br>"Importa lead" |
| Soluzioni dell'organizzazione | Tutti gli utenti dotati di autorizzazione "Importa soluzioni" |
| Oggetti personalizzati dell'organizzazione | Qualsiasi utente con autorizzazione "Importa oggetti personalizzati" |

### Importazione guidata di membri campagna

| Record da importare | Autorizzazione necessaria |
|---|---|
| Nuovi membri campagna (Importazione guidata dati) | "Modifica" per le campagne<br>E<br>casella `Utente marketing` selezionata nelle informazioni utente<br>E<br>"Importa lead" |

| Record da importare | Autorizzazione necessaria |
| --- | --- |
| Membri campagna aggiornati (Aggiornamento guidato campagna) | "Modifica" per le campagne<br>E<br>"Importa lead"<br>E<br>"Lettura" per i referenti<br>casella `Utente marketing` selezionata nelle informazioni utente |

Importante: Salesforce ha sostituito le singole procedure di importazione guidata per account, referenti e altri oggetti con una procedura unificata di Importazione guidata dati (le singole procedure di importazione guidata si aprono in piccole finestre popup, mentre l'importazione unificata si apre in un browser di dimensioni normali con dataimporter.app alla fine dell'URL). Per iniziare a utilizzare la procedura unificata, da Imposta, immettere *`Importazione guidata dati`* nella casella `Ricerca veloce`, quindi selezionare **Importazione guidata dati**. (le opzioni visualizzate dipendono dalle autorizzazioni di cui si dispone).

## Quali formati di file possono essere gestiti dall'importazione guidata?

È possibile importare referenti e account aziendali direttamente da un file di ACT! o di Outlook o da qualsiasi file CSV, quale un file GoldMine o Excel. È possibile importare lead, soluzioni, oggetti personalizzati o account personali da qualsiasi file CSV.

Nota: se le virgole non sono appropriate per le proprie impostazioni internazionali, utilizzare la tabulazione o un altro delimitatore.

## Quali dati possono essere importati?

Le procedure di importazione guidata possono essere utilizzate per importare i record seguenti:

**Referenti e account aziendali**

Utilizzare la procedura guidata di importazione dei referenti personali e l'importazione guidata dei dati per importare referenti e account aziendali.

Nelle organizzazioni che utilizzano le versioni Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition e Developer Edition è inoltre possibile importare note relative ad account aziendali e referenti.

**Account personali**

Nelle organizzazioni che utilizzano le versioni Enterprise Edition, Unlimited Edition, Performance Edition e Developer Edition, utilizzare la procedura guidata Importa account personali per importare gli account personali di cui si è titolari. Gli amministratori possono utilizzare la procedura guidata Importa account personali dell'organizzazione per importare gli account personali di più utenti.

**Lead**

La procedura Importazione guidata dati consente di importare lead nelle organizzazioni che utilizzano le versioni Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition e Developer Edition.

**Soluzioni**

La procedura Importazione guidata dati consente di importare soluzioni nelle organizzazioni che utilizzano le versioni Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition e Developer Edition.

**Oggetti personalizzati**

La procedura Importazione guidata dati consente di importare gli oggetti personalizzati nelle organizzazioni che utilizzano le versioni Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition e Developer Edition.

Nell'importazione guidata dei dati per account, referenti, lead, soluzioni e oggetti personalizzati, gli amministratori possono eseguire l'importazione in qualsiasi campo indicato, anche se il campo è nascosto o di sola lettura nel relativo layout di pagina o nelle impostazioni di protezione a livello di campo. I singoli utenti possono importare solo i campi che sono loro accessibili tramite il rispettivo layout di pagina o le impostazioni di protezione a livello di campo.

Non sono disponibili importazioni di altri record.

Importante: Salesforce ha sostituito le singole procedure di importazione guidata per account, referenti e altri oggetti con una procedura unificata di Importazione guidata dati (le singole procedure di importazione guidata si aprono in piccole finestre popup, mentre l'importazione unificata si apre in un browser di dimensioni normali con dataimporter.app alla fine dell'URL). Per iniziare a utilizzare la procedura unificata, da Imposta, immettere *Importazione guidata dati* nella casella `Ricerca veloce`, quindi selezionare **Importazione guidata dati**. (le opzioni visualizzate dipendono dalle autorizzazioni di cui si dispone).

## Esistono limitazioni delle dimensioni dei dati delle importazioni?

Sì. I file di importazione non possono superare i 100 MB, e i singoli record all'interno del file non possono superare i 400 kB. Inoltre, ogni nota e descrizione importata non può avere dimensioni superiori a 32 kB. Le descrizioni più lunghe di 32 kB vengono troncate.

Oltre ai limiti del file di importazione, l'importazione è soggetta anche ai limiti di memoria complessivi dell'organizzazione. Tenere presente che le dimensioni del file di importazione non corrispondono esattamente allo spazio di memoria necessario per quei record. Ad esempio, un file di importazione di 50 MB non crea necessariamente 50 MB di dati in Salesforce.

Importante: Salesforce ha sostituito le singole procedure di importazione guidata per account, referenti e altri oggetti con una procedura unificata di Importazione guidata dati (le singole procedure di importazione guidata si aprono in piccole finestre popup, mentre l'importazione unificata si apre in un browser di dimensioni normali con dataimporter.app alla fine dell'URL). Per iniziare a utilizzare la procedura unificata, da Imposta, immettere *Importazione guidata dati* nella casella `Ricerca veloce`, quindi selezionare **Importazione guidata dati**. (le opzioni visualizzate dipendono dalle autorizzazioni di cui si dispone).

## Perché non riesco ad accedere a Data Loader?

In caso di problemi nell'accedere a Data Loader, provare le seguenti soluzioni.

- Aggiungere una chiave di protezione alla fine della password di accesso a Data Loader.
- Modificare il `Server host` in modo che punti al server desiderato in Data Loader con la procedura seguente:
  1. Avviare Data Loader.
  2. Selezionare **Settings** > **Settings**.
  3. Impostare `Server host` su `https://`*`nome_istanza`*`.salesforce.com`, dove *`nome_istanza`* è l'istanza di Salesforce in uso.
  4. Fare clic su **OK** per salvare le impostazioni.
- Chiedere all'amministratore se è stato impostato un server proxy. In caso affermativo, modificare di conseguenza le impostazioni di Data Loader. Se si utilizzano API dietro un server proxy, questo impedisce alle API di collegarsi ai server di Salesforce; nella Cronologia accessi non saranno presenti informazioni sulle API.
- Provare ad accedere su un altro computer per verificare che il problema non sia causato dalle impostazioni del proprio dispositivo locale.

## Perché Data Loader non importa i caratteri speciali?

Se Data Loader non riesce a importare caratteri speciali come ö, ñ o é, è possibile che il file dei dati di origine non abbia una codifica corretta. Per fare in modo che il file sia codificato correttamente:

1. Apportare eventuali modifiche al file di dati di origine in formato .xls.
2. In Microsoft® Excel®, salvare una copia del file come Testo Unicode.
3. Aprire il file di Testo Unicode appena salvato con un editor di testo.
4. Fare clic su **File** > **Salva con nome** per modificare le seguenti impostazioni del file:
   - Estensione del file — `.csv`
   - Tipo di salvataggio — **Tutti i file**
   - Codifica — **UTF-8**
5. Fare clic su **Salva** e chiudere il file.

   Nota: Non aprire il file dopo avere salvato le impostazioni per non rischiare di annullare le modifiche apportate alla codifica.
6. Importare normalmente i dati con Data Loader e selezionare il file .csv appena creato.

## È possibile eseguire importazioni nei campi personalizzati?

Sì. Prima dell'importazione, l'amministratore deve creare i campi personalizzati.

Per i campi casella di controllo, i record con valore *1* vengono importati con il segno di spunta e quelli con valore *0* senza segno di spunta.

VEDERE ANCHE:

Panoramica sull'importazione

## È possibile eseguire importazioni in campi che non si trovano nel layout di pagina personale?

No. È possibile importare solo nei campi a cui si può accedere tramite il proprio layout di pagina o le impostazioni di protezione a livello di campo. Tuttavia, nelle importazioni guidate di account, referenti, lead, soluzioni e oggetti personalizzati dell'organizzazione, gli amministratori possono eseguire l'importazione in qualsiasi campo elencato, anche se il campo è nascosto o di sola lettura nel loro layout di pagina o nelle impostazioni di protezione a livello di campo.

Importante: Salesforce ha sostituito le singole procedure di importazione guidata per account, referenti e altri oggetti con una procedura unificata di Importazione guidata dati (le singole procedure di importazione guidata si aprono in piccole finestre popup, mentre l'importazione unificata si apre in un browser di dimensioni normali con dataimporter.app alla fine dell'URL). Per iniziare a utilizzare la procedura unificata, da Imposta, immettere *`Importazione guidata dati`* nella casella `Ricerca veloce`, quindi selezionare **Importazione guidata dati**. (le opzioni visualizzate dipendono dalle autorizzazioni di cui si dispone).

## Posso importare dati in un campo elenco di selezione se i valori non corrispondono?

Si consiglia di importare i dati in un elenco di selezione esistente quando questo rappresenta con precisione i dati, anche se i valori esatti non corrispondono. Le procedure guidate di importazione avvertono l'utente prima di importare nuovi valori negli elenchi di selezione. Tuttavia, per i campi elenco di selezione esse accettano qualsiasi valore, anche non predefinito. In un secondo momento, l'amministratore potrà modificare l'elenco di selezione per aggiungervi i valori necessari. Si noti che le procedure guidate di importazione non consentono di importare più di 100 nuovi valori di elenco di selezione o di elenco di selezione a selezione multipla per qualsiasi campo nel corso di un'unica importazione.

**Importante:** Salesforce ha sostituito le singole procedure di importazione guidata per account, referenti e altri oggetti con una procedura unificata di Importazione guidata dati (le singole procedure di importazione guidata si aprono in piccole finestre popup, mentre l'importazione unificata si apre in un browser di dimensioni normali con dataimporter.app alla fine dell'URL). Per iniziare a utilizzare la procedura unificata, da Imposta, immettere *Importazione guidata dati* nella casella `Ricerca veloce`, quindi selezionare **Importazione guidata dati**. (le opzioni visualizzate dipendono dalle autorizzazioni di cui si dispone).

## È possibile eliminare i dati importati se si commette un errore?

L'amministratore può, da Imposta, immettere *Eliminazione globale record* nella casella `Ricerca veloce`, quindi selezionare **Eliminazione globale record** per eseguire un'eliminazione globale di account, referenti, lead o soluzioni importati per errore. Non è possibile eliminare tutti gli oggetti personalizzati importati per errore.

È possibile annullare l'importazione dell'organizzazione nell'Area di attesa importazione se non è ancora stata avviata l'elaborazione. Da Imposta, immettere *Importazioni* nella casella `Ricerca veloce`, quindi selezionare **Importazioni**. L'area di attesa importazione non è accessibile nelle organizzazioni che utilizzano la versione Personal Edition.

## Come si aggiornano i record con l'importazione guidata dei dati?

È possibile aggiornare lead, referenti o account mediante l'Importazione guidata dati utilizzando l'ID del record come identificatore univoco. Questa procedura non è valida per gli oggetti personalizzati.

**Nota:** La procedura presuppone una conoscenza di Salesforce di un livello da amministratore.

Prima di iniziare, preparare i dati da aggiornare.

1. Creare un rapporto tabulare per i record da aggiornare, inserendovi l'ID dei record e i campi da aggiornare.
2. Salvare il rapporto in locale come file .csv per avere una copia di backup.
3. Fare clic su **Salva con nome** per creare una nuova versione del file .csv e apportare le modifiche desiderate ai dati.
4. Fare clic su **Salva**.

Dopo avere aggiornato il rapporto, importare il file .csv in Salesforce. La procedura varia a seconda dei record da aggiornare.

### Per aggiornare i lead

1. Da Imposta, immettere *Importazione guidata dati* nella casella `Ricerca veloce`, selezionare **Importazione guidata dati**, quindi fare clic su **Lancia l'importazione guidata!**.
2. Fare clic su **Lead**.
3. Fare clic su **Aggiorna i record esistenti**.
4. In Tipo corrispondente, scegliere **ID Salesforce**. Fare clic su **Avanti**.
5. Selezionare **Sovrascrivere valori di lead esistenti**.
6. Mappare il campo `ID lead` alla colonna ID lead del file locale e mappare tutti gli altri campi.
7. Controllare le modifiche apportate e fare clic su **Importa ora**.

### Per aggiornare account o referenti

1. Da Imposta, immettere *Importazione guidata dati* nella casella `Ricerca veloce`, selezionare **Importazione guidata dati**, quindi fare clic su **Lancia l'importazione guidata!**.
2. Fare clic su **Account e referenti**.

3. Fare clic su **Aggiorna i record esistenti**.
4. In Tipo corrispondente referente, scegliere **ID Salesforce**. Il Tipo corrispondente account viene abbinato automaticamente al Tipo corrispondente referente. Fare clic su **Avanti**.
5. Mappare il campo `ID referente` alla colonna ID referente del file locale e mappare gli altri campi referente. Fare clic su **Avanti**.
6. Mappare i campi telefono e indirizzo referente. Fare clic su **Avanti**.
7. Selezionare **Sovrascrivere valori di account esistenti**, mappare il campo `ID account` alla colonna ID account del file locale e mappare gli altri campi account.
8. Caricare il file CSV che si sta importando.
9. Mappare i campi di importazione aggiuntivi e fare clic su **Avanti**.
10. Fare clic su **Importa ora**.

La procedura Importazione guidata dati abbina gli ID dei record presenti nel file agli ID dei record di Salesforce e aggiorna i campi che sono stati mappati.

## Perché i campi data non vengono importati correttamente quando uso Data Loader?

Quando si importano campi data con Data Loader, può accadere che le date siano esportate in modo errato perché Data Loader converte la data specificata nel file .csv importato in base al fuso orario GMT. Se il fuso orario del computer in uso non è GMT o se il suo orologio tiene conto dell'ora legale, le date potrebbero essere spostate di un giorno.

Per evitare che Data Loader modifichi la data quando la converte sul fuso orario GMT, modificare direttamente il formato delle celle contenenti date secondo il fuso orario locale di origine.

1. Aprire il file .csv in Microsoft® Excel®.
2. In ogni cella in cui è stata inserita una data, aggiungere i dati dell'ora per rappresentare il fuso orario locale. Ad esempio, se la data è 9 giugno 2011 e il fuso orario è GMT+8, inserire *`9 giugno 2011 8:00`*. Excel riformatterà la data in `6/9/2011 8:00`.
3. Fare clic con il pulsante destro del mouse nella cella in cui è stata inserita la data e fare clic su **Formato celle**.
4. Fare clic su **Numero** > **Personalizzato**.
5. In `Tipo`, digitare *`aaaa-mm-ggThh:mm:ss.sssZ`*. Ad esempio, se la cella era *`6/9/2011 8:00`*, ora sarà `2011-06-09T08:00:00.00Z`.

## Che cosa visualizza l'area di attesa di importazione?

Da Imposta, immettere *`Importazioni`* nella casella `Ricerca veloce`, quindi selezionare **Importazioni**. L'area di attesa importazione mostra tutti i file non elaborati che sono stati inviati utilizzando la procedura guidata di importazione dei dati in Imposta. È possibile vedere quando sono stati inviati i singoli file, il loro stato e una stima del tempo necessario per l'elaborazione. Per annullare l'importazione dei file non ancora in corso di elaborazione, fare clic su **Canc**. L'area di attesa importazione non è accessibile nelle organizzazioni che utilizzano la versione Personal Edition.

Importante: Salesforce ha sostituito le singole procedure di importazione guidata per account, referenti e altri oggetti con una procedura unificata di Importazione guidata dati (le singole procedure di importazione guidata si aprono in piccole finestre popup, mentre l'importazione unificata si apre in un browser di dimensioni normali con dataimporter.app alla fine dell'URL). Per iniziare a utilizzare la procedura unificata, da Imposta, immettere *`Importazione guidata dati`* nella casella `Ricerca veloce`, quindi selezionare **Importazione guidata dati**. (le opzioni visualizzate dipendono dalle autorizzazioni di cui si dispone).

## Quanto tempo richiede l'importazione di un file?

Per le importazioni guidate eseguite dai singoli utenti, il tempo necessario dipende dal volume dei dati, ma in media sono sufficienti pochi minuti.

Le importazioni guidate per gli amministratori funzionano in modo asincrono e, una volta completata l'importazione di un file, si riceve un'email di notifica. L'importazione asincrona può richiedere da pochi minuti a un massimo di 24 ore.

Tranne che nella versione Personal Edition, gli amministratori possono inoltre controllare l'area di attesa di importazione per verificare l'andamento del processo. Da Imposta, immettere *Importazioni* nella casella Ricerca veloce, quindi selezionare **Importazioni**. Per velocizzare il processo di importazione, si consiglia di leggere le relative istruzioni nella sezione Panoramica sull'importazione a pagina 338.

Importante: Salesforce ha sostituito le singole procedure di importazione guidata per account, referenti e altri oggetti con una procedura unificata di Importazione guidata dati (le singole procedure di importazione guidata si aprono in piccole finestre popup, mentre l'importazione unificata si apre in un browser di dimensioni normali con dataimporter.app alla fine dell'URL). Per iniziare a utilizzare la procedura unificata, da Imposta, immettere *Importazione guidata dati* nella casella Ricerca veloce, quindi selezionare **Importazione guidata dati**. (le opzioni visualizzate dipendono dalle autorizzazioni di cui si dispone).

## Perché l'importazione di un file può comportare un ritardo?

Per controllare il volume delle importazioni e garantire le massime prestazioni a tutti gli utenti, i file di importazione delle organizzazioni vengono accettati in modalità "asincrona". I file transitano perciò in un'area di attesa controllata e vengono importati nel momento in cui il sistema è in grado di gestire i dati in modo ottimale. Tuttavia, l'importazione dell'organizzazione non richiede mai più di 24 ore. Al termine dell'importazione viene inviata un'email di notifica.

## È possibile importare totali in più valute?

Se un'organizzazione con Group Edition, Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition o Developer Edition ha impostato la funzione che consente di utilizzare più valute, è possibile importare gli importi in valute diverse utilizzando la colonna Codice ISO valuta nel file di importazione.

## L'assistenza clienti può fornire un supporto per l'importazione dei dati personali?

L'Assistenza clienti è disponibile per assistere le organizzazioni che utilizzano le versioni Group Edition, Contact Manager Edition, Professional Edition, Enterprise Edition, Unlimited Edition e Performance Edition nel processo di importazione.

## È possibile importare i dati in più di una lingua?

L'importazione guidata consente di importare una sola lingua alla volta, ovvero la lingua dell'utente che effettua l'importazione. Se si dispone degli stessi dati in lingue diverse, eseguire un'importazione per ciascuna lingua aggiuntiva.

Importante: Salesforce ha sostituito le singole procedure di importazione guidata per account, referenti e altri oggetti con una procedura unificata di Importazione guidata dati (le singole procedure di importazione guidata si aprono in piccole finestre popup, mentre l'importazione unificata si apre in un browser di dimensioni normali con dataimporter.app alla fine dell'URL). Per iniziare a utilizzare la procedura unificata, da Imposta, immettere *Importazione guidata dati* nella casella Ricerca veloce, quindi selezionare **Importazione guidata dati**. (le opzioni visualizzate dipendono dalle autorizzazioni di cui si dispone).

## Come si eseguono gli aggiornamenti globali dei record?

Per aggiornare più di 50.000 ma meno di 5 milioni di record, utilizzare Data Loader.

Per aggiornare più di 5 milioni di record, si consiglia di collaborare con un partner Salesforce o di visitare il sito *App Exchange* per verificare la disponibilità di un prodotto partner adatto.

### Come si aggiornano i campi con valori vuoti?

Per sostituire i campi con valori nulli è necessario utilizzare Data Loader.

1. Scegliere **Start** > **Tutti i programmi** > **Salesforce** > **Data Loader** > **Data Loader** per aprire Data Loader.
2. Fare clic su **Export** e completare la procedura guidata. Al termine dell'operazione, fare clic su **View Extraction**.
3. Fare clic su **Open in external program** per aprire i dati in Excel. Cancellare i valori dai campi da aggiornare.
4. In Data Loader, scegliere **Settings** > **Settings** e selezionare **Insert null values**. Fare clic su **OK** per salvare le impostazioni.
5. Fare clic su **Update** e seguire la procedura guidata per reimportare i dati.

### Cos'è l'ID esterno?

Quando si importano oggetti personalizzati, soluzioni o account personali, è possibile utilizzare ID esterni per impedire la creazione di record duplicati durante l'importazione.

Un ID esterno è un campo personalizzato che possiede l'attributo "ID esterno", ovvero contiene identificatori univoci di record di un sistema esterno a Salesforce. Quando si seleziona questa opzione, l'importazione guidata rileverà i record esistenti in Salesforce che sono associati allo stesso ID esterno. Per questa operazione non è rilevante la distinzione tra maiuscole e minuscole, ossia "ABC" corrisponde ad "abc". Esiste però un'eccezione: se il campo personalizzato possiede l'attributo "Univoco" e se è selezionata l'opzione per la distinzione tra maiuscole e minuscole, le lettere maiuscole e minuscole non saranno considerate identiche.

## Importazione di account personali

- Come è possibile evitare la creazione di account personali duplicati?
- È necessario sincronizzare Outlook o utilizzare le importazioni guidate per caricare i dati in Salesforce?
- Come è possibile utilizzare l'importazione guidata per effettuare un aggiornamento globale degli account personali esistenti?
- Quali campi account personale sono richiesti per l'importazione?
- È possibile aggiornare i campi di ricerca per gli account personali?

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

### Come è possibile evitare la creazione di account personali duplicati?

Per evitare che vengano creati record account personali duplicati durante l'importazione, compilare una colonna del file di importazione con i nomi, gli indirizzi email, gli ID Salesforce o gli ID esterni degli account personali. Questi sono i campi che possono essere utilizzati per individuare la corrispondenza tra le righe nel file di importazione e i record esistenti in Salesforce. Nella procedura guidata è possibile specificare il campo utilizzato per l'individuazione della corrispondenza dei record e le azioni da intraprendere quando viene rilevato un record corrispondente.

Importante: Salesforce ha sostituito le singole procedure di importazione guidata per account, referenti e altri oggetti con una procedura unificata di Importazione guidata dati (le singole procedure di importazione guidata si aprono in piccole finestre popup, mentre l'importazione unificata si apre in un browser di dimensioni normali con dataimporter.app alla fine dell'URL). Per iniziare a utilizzare la procedura unificata, da Imposta, immettere *`Importazione guidata dati`* nella casella `Ricerca veloce`, quindi selezionare **Importazione guidata dati**. (le opzioni visualizzate dipendono dalle autorizzazioni di cui si dispone).

## Come è possibile utilizzare l'importazione guidata per effettuare un aggiornamento globale degli account personali esistenti?

Per eseguire l'aggiornamento globale dei record di account personali esistenti mediante l'importazione guidata:

1. Eseguire un rapporto account personale ed esportare i risultati in Excel. Per attivare l'individuazione di corrispondenze tra i record, includere il campo nome, indirizzo email, ID Salesforce o ID esterno nel rapporto.
2. Utilizzare Excel o un'applicazione analoga per aggiornare i valori dei campi nel file di importazione in base alle esigenze
3. Avviare l'importazione guidata appropriata.
   - Se si è titolari dei record nel file di importazione, avviare l'importazione guidata degli account personali dalle proprie impostazioni selezionando **Importa** > **Importa account personali**.
   - Se i record nel file di importazione sono di proprietà di più utenti diversi, avviare la procedura guidata Importa account personali dell'organizzazione da Imposta, immettendo "Importa account personali" nella casella `Ricerca veloce` e selezionando **Importa account personali**.
4. Al passaggio Impedire i duplicati:
   - Se si utilizza la procedura guidata Importa account personali dell'organizzazione, selezionare il pulsante di opzione `Sì`. Questa opzione non è disponibile nelle altre importazioni guidate.
   - Nella sezione “Quali sono i campi...”, selezionare il campo del file da utilizzare per la corrispondenza dei record: nome, ID Salesforce, indirizzo email o ID esterno.
   - Nella sezione relativa ai record esistenti, scegliere la seconda opzione, `Aggiorna record esistenti e non inserire nuovi record`.
5. Continuare con le altre fasi della procedura guidata.
6. Al termine della procedura guidata e dopo avere ricevuto la notifica della conclusione dell'elaborazione, verificare in Salesforce che i record siano stati aggiornati come previsto.

Importante: Salesforce ha sostituito le singole procedure di importazione guidata per account, referenti e altri oggetti con una procedura unificata di Importazione guidata dati (le singole procedure di importazione guidata si aprono in piccole finestre popup, mentre l'importazione unificata si apre in un browser di dimensioni normali con dataimporter.app alla fine dell'URL). Per iniziare a utilizzare la procedura unificata, da Imposta, immettere *`Importazione guidata dati`* nella casella `Ricerca veloce`, quindi selezionare **Importazione guidata dati**. (le opzioni visualizzate dipendono dalle autorizzazioni di cui si dispone).

## Quali campi account personale sono richiesti per l'importazione?

Ogni account personale contiene un campo nome che deve essere incluso nel file di importazione. Inoltre, se l'amministratore ha definito campi personalizzati universalmente obbligatori per gli account personali, anche quei campi devono essere inclusi nel file di importazione.

## È possibile aggiornare i campi di ricerca per gli account personali?

Sì, se gli account personali hanno una relazione di ricerca con un altro oggetto, è possibile utilizzare l'importazione guidata per aggiornare il valore di tale campo di ricerca. Si consiglia di effettuare la procedura seguente:

1. Eseguire un rapporto account personale ed esportare i risultati in Excel. Includere nel rapporto gli ID Salesforce dell'account personale e dell'oggetto cui viene fatto riferimento nel campo di ricerca.
2. Utilizzare Excel o un'applicazione analoga per aggiornare i valori dei campi nel file di importazione in base alle esigenze
3. Avviare la procedura guidata Importa account personali dell'organizzazione da Imposta, immettendo "Importa account personali" nella casella `Ricerca veloce` e selezionando **Importa account personali**.
4. Al passaggio Impedire i duplicati:

- Scegliere il pulsante di opzione `Sì`.
- Scegliere `ID Salesforce`.
- L'opzione `Aggiorna record esistenti e non inserire nuovi record` è selezionata automaticamente perché si sta effettuando una ricerca di corrispondenza in base all'ID Salesforce.

5. Al passaggio Specificare le relazioni:
   - Specificare il campo relativo al titolare del record nel file di importazione.
   - Selezionare la casella corrispondente al campo di ricerca che si sta includendo nel file di importazione.

6. Al passaggio Definire le corrispondenze di ricerca, scegliere `ID Salesforce`.

   Nota: i record correlati devono essere già presenti in Salesforce prima di procedere. I record correlati non verranno aggiornati durante l'importazione, anche se il file di importazione contiene valori diversi per i campi presenti in tali record correlati.

7. Al termine della procedura guidata e dopo avere ricevuto la notifica della conclusione dell'elaborazione, verificare in Salesforce che i record account personali siano stati aggiornati come previsto.

Importante: Salesforce ha sostituito le singole procedure di importazione guidata per account, referenti e altri oggetti con una procedura unificata di Importazione guidata dati (le singole procedure di importazione guidata si aprono in piccole finestre popup, mentre l'importazione unificata si apre in un browser di dimensioni normali con dataimporter.app alla fine dell'URL). Per iniziare a utilizzare la procedura unificata, da Imposta, immettere *`Importazione guidata dati`* nella casella `Ricerca veloce`, quindi selezionare **Importazione guidata dati**. (le opzioni visualizzate dipendono dalle autorizzazioni di cui si dispone).

# Importazione di membri della campagna

- Per quale motivo sono presenti due importazioni guidate campagna?
- Quanti membri campagna è possibile importare?
- Chi può importare i membri campagna?
- Quale stato viene assegnato ai membri campagna?
- Come si prepara il file di importazione campagna?

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

## Per quale motivo sono presenti due importazioni guidate campagna?

Per accedere alle importazioni guidate campagna è possibile utilizzare i link **Aggiungi membri - Importa file** e **Aggiorna e aggiungi membri - Importa file** nella pagina **Gestisci membri** disponibile da qualsiasi pagina di dettagli delle campagne. Le procedure guidate sono le seguenti:

- **Importazione guidata dati**: Per accedere a questa procedura guidata dalla pagina dei dettagli di una campagna, fare clic su **Gestisci membri** > **Aggiungi membri - importa file** > **Lead**. Utilizzare questa procedura guidata per importare i lead. Consente di importare un elenco di nomi, creare o aggiornare lead nel sistema e associarli alla campagna.
- **Aggiornamento guidato campagna**: Per accedere a questa procedura guidata dalla pagina dei dettagli di una campagna, fare clic su **Gestisci membri** > **Aggiorna e aggiungi membri - Importa file** > **Aggiorna e aggiungi membri campagna**. Utilizzare questa procedura guidata per aggiornare lo stato membro campagna dei lead e referenti esistenti. Consente di importare un elenco di referenti e lead esistenti di Salesforce, associarli alla campagna e aggiornare la relativa cronologia delle risposte.

## Quanti membri campagna è possibile importare?

Il numero di membri campagna che è possibile importare è stabilito dalle seguenti procedure guidate:

- **Importazione guidata lead**: importa fino a 50.000 lead alla volta.

- **Aggiornamento guidato campagna**: aggiorna fino a 50.000 referenti e lead esistenti alla volta.

Oltre al limite di record, l'importazione è soggetta anche ai limiti di memoria complessivi dell'organizzazione.

Importante: Salesforce ha sostituito le singole procedure di importazione guidata per account, referenti e altri oggetti con una procedura unificata di Importazione guidata dati (le singole procedure di importazione guidata si aprono in piccole finestre popup, mentre l'importazione unificata si apre in un browser di dimensioni normali con dataimporter.app alla fine dell'URL). Per iniziare a utilizzare la procedura unificata, da Imposta, immettere *Importazione guidata dati* nella casella Ricerca veloce, quindi selezionare **Importazione guidata dati**. (le opzioni visualizzate dipendono dalle autorizzazioni di cui si dispone).

## Chi può importare i membri campagna?

Per utilizzare l'importazione guidata dati per importare nuovi lead per una campagna o le procedure guidate di importazione delle campagne per aggiornare la cronologia della campagna per più lead e referenti, gli utenti devono avere la casella Utente marketing selezionata nelle relative informazioni personali. Devono inoltre disporre del profilo Utente marketing oppure delle autorizzazioni "Importa lead" e "Modifica" per le campagne.

## Quale stato viene assegnato ai membri campagna?

Con le importazioni guidate campagna, è possibile assegnare uno stato membro campagna a un lead o a un referente in uno dei due modi seguenti:

- Aggiungere una colonna Stato al file di importazione. Immettere lo stato per ciascun lead o referente della campagna.
- Selezionare uno stato predefinito nell'importazione guidata campagna. A qualsiasi lead o referente con uno stato vuoto o non valido nel file di importazione verrà automaticamente assegnato lo stato predefinito.

Importante: Salesforce ha sostituito le singole procedure di importazione guidata per account, referenti e altri oggetti con una procedura unificata di Importazione guidata dati (le singole procedure di importazione guidata si aprono in piccole finestre popup, mentre l'importazione unificata si apre in un browser di dimensioni normali con dataimporter.app alla fine dell'URL). Per iniziare a utilizzare la procedura unificata, da Imposta, immettere *Importazione guidata dati* nella casella Ricerca veloce, quindi selezionare **Importazione guidata dati**. (le opzioni visualizzate dipendono dalle autorizzazioni di cui si dispone).

## Come si prepara il file di importazione campagna?

Il file di importazione campagna si può preparare mediante una delle seguenti procedure guidate:

- **Importazione guidata lead**: prepara il file di importazione dei nuovi lead mediante Excel.
- **Aggiornamento guidato campagna**: aggiorna solo lo stato membro di un lead o di un referente esistente. Il file di importazione deve contenere una colonna Stato oltre a una colonna ID record che riporti i valori univoci ID referente o ID lead di Salesforce per lead e referenti.

Importante: Salesforce ha sostituito le singole procedure di importazione guidata per account, referenti e altri oggetti con una procedura unificata di Importazione guidata dati (le singole procedure di importazione guidata si aprono in piccole finestre popup, mentre l'importazione unificata si apre in un browser di dimensioni normali con dataimporter.app alla fine dell'URL). Per iniziare a utilizzare la procedura unificata, da Imposta, immettere *Importazione guidata dati* nella casella Ricerca veloce, quindi selezionare **Importazione guidata dati**. (le opzioni visualizzate dipendono dalle autorizzazioni di cui si dispone).

# Gestione dei dati

## Esportazione di dati di backup

A seconda della versione utilizzata, l'organizzazione può generare file di backup dei dati su base settimanale o mensile. È possibile esportare tutti i dati dell'organizzazione in un gruppo di file CSV.

Nota: gli utenti che dispongono dell'autorizzazione "Esportazione settimanale" possono vedere tutti i dati esportati e tutti gli oggetti e i campi personalizzati nella pagina Servizio di esportazione. L'autorizzazione è concessa per impostazione predefinita solo al profilo Amministratore di sistema per la grande visibilità consentita.

I file di backup possono essere generati manualmente ogni sei giorni (per l'esportazione settimanale) o ogni 28 giorni (per l'esportazione mensile). Inoltre, è possibile pianificare la generazione automatica dei file di backup a intervalli settimanali o mensili.

La presenza di traffico intenso può ritardare la consegna di un'esportazione. Si supponga ad esempio di aver pianificato l'esecuzione di un'esportazione settimanale fino alla fine del mese, a partire dal 1° aprile. La prima richiesta di esportazione accede all'area di attesa, ma a causa del traffico intenso l'esportazione non viene consegnata fino all'8 aprile. Il 7 aprile, quando è pianificata l'elaborazione della seconda richiesta di esportazione, la prima richiesta si trova ancora nell'area di attesa, pertanto la seconda richiesta non viene elaborata fino al 14 aprile.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Esportazione settimanale disponibile nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

Esportazione mensile disponibile in: **tutte** le versioni tranne Database.com Edition

AUTORIZZAZIONI UTENTE

Per esportare dati:
- "Esportazione settimanale"

1. Da Imposta, immettere *`Esportazione dati`* nella casella `Ricerca veloce`, quindi selezionare **Esportazione dati** e **Esporta ora** o **Pianifica esportazione**.
   - L'opzione **Esporta ora** prepara i file all'esportazione immediata. L'opzione è disponibile solo se dall'ultima esportazione è trascorso un periodo sufficiente.
   - L'opzione **Pianifica esportazione** permette di pianificare il processo di esportazione a intervalli settimanali o mensili.
2. Selezionare la codifica desiderata per il file di esportazione.
3. Selezionare `Includi immagini, documenti e allegati` e `Includi i file Chatter e le versioni dei documenti Salesforce CRM Content` per includere queste voci nei dati dell'esportazione.

   Nota: Se si seleziona `Includi immagini, documenti e allegati` e `Includi i file Chatter e le versioni dei documenti Salesforce CRM Content` aumenta il tempo di elaborazione dell'esportazione dei dati.
4. Selezionare `Sostituisci ritorni a capo con spazi` se si desidera che i file esportati presentino degli spazi anziché ritorni a capo o interruzioni di riga. Questa selezione è utile se si prevede di utilizzare i file di esportazione per l'importazione o per altre integrazioni.
5. Se si pianifica un'esportazione, selezionare la frequenza (disponibile solo per le organizzazioni con esportazioni mensili), le date di inizio e fine e l'ora dell'esportazione.
6. In Dati esportati, selezionare i tipi di dati da includere nell'esportazione. Se non si conosce la terminologia utilizzata per alcuni tipi di dati, si consiglia di selezionare **Includi tutti i dati**. Tenere presente quanto segue:
   - Dalle esportazioni sono sempre esclusi i campi Formula e riepilogo di roll-up.
   - Se l'organizzazione utilizza divisioni, nell'esportazione vengono inclusi i dati di tutte le divisioni.
   - Se l'organizzazione utilizza account personali e si stanno esportando account, tutti i campi account vengono inclusi nei dati degli account.

- Se l'organizzazione utilizza account personali e si stanno esportando referenti, i record account personali vengono inclusi nei dati dei referenti. Tuttavia, i dati dei referenti includono solo i campi condivisi dai referenti e dagli account personali.

7. Fare clic su **Avvia esportazione** oppure su **Salva**.

   Salesforce crea un archivio .zip di file CSV e invia un messaggio email quando questo è pronto. Le esportazioni verranno completate al più presto, tuttavia non possiamo garantire la data e l'ora di completamento. Le esportazioni di grandi dimensioni vengono ripartite in più file. Selezionare il link nel messaggio email o fare clic su **Esportazione dati** per scaricare il file zip. I file zip vengono eliminati 48 ore dopo l'invio del messaggio email. Il limite di tempo delle 48 ore non include i fine settimana; pertanto, se il file da scaricare è pronto il giovedì alle 16:00, non verrà eliminato fino a lunedì alle 16:00.

   Nota: Per motivi di sicurezza, Salesforce potrebbe richiedere agli utenti di superare un test di verifica CAPTCHA per poter esportare i dati dalla propria organizzazione. Questo semplice test impedisce ai programmi dannosi di accedere ai dati della propria organizzazione. Per superare il test, gli utenti devono digitare correttamente le due parole visualizzate nella sovrapposizione all'interno della casella di testo. Tenere presente che le parole immesse nella casella di testo devono essere separate da uno spazio.

A seconda della codifica selezionata, potrebbe essere necessario apportare modifiche al file di esportazione prima di visualizzarlo. Attenersi alle istruzioni seguenti in base alla codifica caratteri selezionata.

## Visualizzazione di file di esportazione codificati Unicode (UTF-8)

Se si dispone di Microsoft Excel 2003:

1. Aprire Microsoft Excel.
2. Fare clic su **File** > **Nuovo**.
3. Fare clic su **Dati** > **Importa dati esterni** > **Importa dati**.
4. Selezionare il file CSV da aprire. Microsoft Excel avvia la procedura guidata per l'importazione di testo.
5. Selezionare “Delimitati” e scegliere l'opzione “Unicode (UTF-8)” come Origine file.
6. Fare clic su **Avanti**.
7. Selezionare “Virgola” nella sezione Delimitatori e fare clic su **Fine**. Potrebbe essere richiesto di selezionare un intervallo di celle.

   Nota: se le virgole non sono appropriate per le proprie impostazioni internazionali, utilizzare la tabulazione o un altro delimitatore.

8. Ripetere la procedura per ogni file.

Se la versione di Microsoft Excel di cui si dispone è antecedente alla versione -2003:

1. Aprire il file in Microsoft Excel.
2. Selezionare **File** > **Salva con nome**.
3. Salvare il file come tipo Pagina Web.
4. Selezionare **Strumenti** > **Opzioni scheda** > **Generale** e fare clic sul pulsante **Opzioni Web**.
5. Selezionare la scheda Codifica, quindi scegliere l'opzione “Unicode (UTF-8)”.
6. Fare clic su **OK** per chiudere le finestre di dialogo.
7. Selezionare **File** > **Salva** per salvare il file con la codifica selezionata.
8. Ripetere la procedura per ogni file.

## Visualizzazione di file di esportazione codificati Unicode (UTF-16, Big Endian)

Aprire i file di esportazione in un editor di testo che supporta questo set di caratteri. Microsoft Excel non supporta questo set di caratteri.

## Visualizzazione di file di esportazione codificati Unicode (Little Endian)

1. Aprire il file in Microsoft Excel.
2. Fare clic sulla colonna A per evidenziare tutta la prima colonna.
3. Aprire il menu **Dati** e scegliere **Testo in colonne**.
4. Selezionare il pulsante di opzione "Delimitati" e fare clic su **Avanti**.
5. Selezionare "Virgola" nella sezione Delimitatori e fare clic su **Fine**.

   Nota: se le virgole non sono appropriate per le proprie impostazioni internazionali, utilizzare la tabulazione o un altro delimitatore.

6. Ripetere la procedura per ogni file.

# Panoramica sul trasferimento di record

Un titolare di record (o qualsiasi utente di livello superiore rispetto al titolare nella gerarchia dei ruoli o dei territori) può trasferire un singolo record a un altro utente. Con alcuni oggetti, quali casi, lead e campagne, è possibile che a un utente venga consentito l'accesso per trasferire record attraverso la condivisione. A seconda del tipo di oggetto, possono esserci diversi modi per trasferire i record a un altro utente:

| Metodo | Disponibile per |
| --- | --- |
| Trasferire un singolo record | Account, campagne, casi, referenti, contratti, lead e oggetti personalizzati |
| Trasferire più record selezionandoli da una visualizzazione elenco e facendo clic su **Cambia titolare** | Casi, lead e oggetti personalizzati che possono appartenere a un utente o a un'area di attesa |
| Trasferire più record utilizzando lo strumento di trasferimento globale | Account, lead e oggetti personalizzati |

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Account, campagne, referenti, contratti, lead e casi non sono disponibili nella versione **Database.com Edition**.

AUTORIZZAZIONI UTENTE

Per trasferire più account, campagne, referenti, contratti e oggetti personalizzati:
- "Trasferisci record"

  E

  "Modifica" per il tipo di oggetto

Per trasferire più lead:
- "Trasferisci lead" o "Trasferisci record"

  E

  "Modifica" per i lead

Per trasferire più casi:
- "Trasferisci casi" O "Trasferisci record"

  E

  "Modifica" per i casi

## Possibilità di modificare la proprietà

- Gli utenti con l'autorizzazione "Modifica tutti i dati" o "Modifica tutto" per l'oggetto in questione possono trasferire qualsiasi record, indipendentemente dal titolare.
- Per trasferire un singolo record o più record da una visualizzazione elenco, il nuovo titolare deve disporre almeno dell'autorizzazione "Lettura" per il tipo di oggetto. La regola non è valida se si utilizza lo strumento di trasferimento globale.
- Per trasferire la proprietà di un singolo record in un'organizzazione che non utilizza la gestione dei territori è necessario disporre dell'autorizzazione "Modifica" appropriata ed essere titolare del record o avere un ruolo superiore a quello del titolare nella gerarchia dei ruoli.

  Ad esempio, per trasferire la proprietà di un account, un utente deve disporre delle autorizzazioni di accesso "Lettura" e "Modifica". Inoltre, il nuovo titolare del record deve avere almeno l'autorizzazione "Lettura" per gli account.

  Le impostazioni di condivisione Accesso completo pubblico e Lettura/Scrittura/Trasferimento pubblico offrono a tutti gli utenti la possibilità di trasferire la proprietà di tale tipo di record a condizione che dispongano dell'autorizzazione "Modifica" appropriata.
- Nelle organizzazioni che utilizzano la gestione dei territori, gli utenti assegnati a territori possono essere abilitati al trasferimento degli account presenti nei propri territori, anche se non sono titolari dei record.
- Per trasferire campagne, gli utenti devono inoltre avere la casella di controllo `Utente Marketing` selezionata nel proprio record utente.

## Modifica della proprietà per gli account del portale

- Per trasferire un account partner, è necessario disporre dell'autorizzazione "Gestisci utenti" o "Gestisci utenti esterni".

- Se l'utente è il titolare di un account Portale Clienti e desidera trasferire l'account, potrà trasferirlo a qualsiasi utente che abbia il suo stesso ruolo senza che siano necessarie autorizzazioni speciali. Un account del Portale Clienti non può essere trasferito a un utente con un ruolo di livello superiore o inferiore.
- Gli account partner possono essere trasferiti solo agli utenti dotati dell'autorizzazione “Gestisci utenti esterni”.
- Per trasferire un account del portale con utenti del Portale Clienti e del Portale partner, è necessario disporre dell'autorizzazione “Gestisci utenti”.
- Non è possibile assegnare un account con utenti del Portale Clienti a un titolare che è utente partner.

VEDERE ANCHE:

Trasferimento globale di record

# Trasferimento globale di record

Utilizzare lo strumento di trasferimento globale per trasferire più account, lead, contratti di servizio e oggetti personalizzati da un utente all'altro.

Nota: per trasferire eventuali record di cui non si è titolari, è necessario disporre delle autorizzazioni utente richieste e dell'accesso di condivisione lettura per i record.

1. Da Imposta, immettere *Trasferimento globale record* nella casella Ricerca veloce, quindi selezionare **Trasferimento globale record**.
2. Fare clic sul link per il tipo di record da trasferire.
3. Se si desidera, specificare il nome del titolare del record esistente nel campo Trasferisci da. Per i lead, è possibile trasferire da utenti o aree di attesa.
4. Nel campo Trasferisci a, digitare il nome del nuovo titolare del record. Per i lead, è possibile trasferire a utenti o aree di attesa.
5. Se l'organizzazione utilizza divisioni, selezionare la casella di controllo Cambia divisione... per impostare la divisione di tutti i record trasferiti sulla divisione predefinita del nuovo titolare.
6. Quando si trasferiscono account, è possibile:
   - Selezionare Trasferisci le opportunità aperte non appartenenti al titolare dell'account esistente per trasferire le opportunità aperte di cui sono titolari altri utenti associati all'account.
   - Selezionare Trasferisci opportunità chiuse per trasferire le opportunità chiuse associate all'account. Tale opzione si applica solo alle opportunità chiuse di proprietà del titolare dell'account; le opportunità chiuse di proprietà di altri utenti non vengono modificate.
   - Selezionare Trasferisci i casi aperti appartenenti al titolare dell'account esistente per trasferire i casi aperti di cui è titolare il titolare dell'account esistente e che sono associati all'account.
   - Selezionare Trasferisci casi chiusi per trasferire i casi chiusi di cui è titolare il titolare dell'account esistente e che sono associati all'account.
   - Selezionare Mantieni team account per mantenere il team account esistente associato all'account. Deselezionare questa casella di controllo per rimuovere il team account esistente associato all'account.
   - Selezionare Mantieni team opportunità su tutte le opportunità per mantenere il team esistente sulle opportunità associate a questo account. Tutte le ripartizioni delle opportunità vengono mantenute e le percentuali di ripartizione assegnate al titolare precedente vengono trasferite al nuovo titolare. Se questa casella non è selezionata, tutti i membri del team opportunità e le ripartizioni vengono eliminati quando l'opportunità viene trasferita.

     Nota: Se si trasferiscono opportunità chiuse, il team opportunità viene mantenuto, indipendentemente da questa impostazione.
7. Inserire i criteri di ricerca che devono essere rispettati dai record da trasferire.
8. Fare clic su **Trova**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Account, Contratti di servizio e Lead non sono disponibili nella versione **Database.com Edition**.

AUTORIZZAZIONI UTENTE

Per eseguire un trasferimento globale di account e contratti di servizio:
- "Trasferisci record"

  E

  "Modifica" per il tipo di oggetto

  E

  "Trasferisci lead"

Per eseguire un trasferimento globale di oggetti personalizzati:
- "Trasferisci record"

  E

  "Modifica" per il tipo di oggetto

Per trasferire globalmente i lead:
- "Trasferisci lead" o "Trasferisci record"

  E

  "Modifica" per i lead

9. Selezionare la casella di controllo accanto ai record da trasferire. Se si desidera, selezionare la casella nell'intestazione di colonna per selezionare tutti i record correntemente visualizzati.

   Nota: se vengono trovati record duplicati, è necessario selezionare solo uno dei record per il trasferimento. Il trasferimento di record duplicati genera un errore.

   I record duplicati possono essere visualizzati se si filtrano i lead in base allo Stato membro campagna e un lead corrispondente ha lo stesso stato membro della campagna su più campagne. Ad esempio, se si specifica *Stato membro campagna uguale a Inviato* e un lead corrispondente, denominato John Smith, ha lo stato Inviato su due campagne, il suo record verrà visualizzato due volte.

10. Fare clic su **Trasferisci**.

VEDERE ANCHE:

Panoramica sul trasferimento di record

# Eliminazione di più record e rapporti

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

Questa funzionalità è disponibile solo nella versione **Database.com Edition** mediante API. È possibile solo effettuare l'eliminazione globale dei record di oggetti personalizzati nella versione **Database.com Edition**.

AUTORIZZAZIONI UTENTE

Per eliminare globalmente dati:

- "Modifica tutti i dati"

È possibile eliminare più rapporti o record contemporaneamente.

I tipi di record per i quali è possibile effettuare l'eliminazione globale includono casi, soluzioni, account, referenti, lead, prodotti e attività.

Di seguito sono riportate alcune situazioni in cui può essere utile procedere all'eliminazione globale.

- Sono stati individuati più rapporti che non vengono più utilizzati e si desidera alleggerire l'elenco dei rapporti sulla scheda Rapporti.
- Sono stati importati i lead dell'organizzazione in modo non corretto e si desidera ricominciare.
- Un utente che ha recentemente lasciato l'organizzazione possedeva referenti che erano duplicati di dati di altri utenti e si desidera eliminare tali referenti duplicati.
- L'organizzazione era solita inserire i lead come referenti con il campo `Tipo` impostato su "Cliente potenziale". Si desidera ora convertire tali account in lead.

  Suggerimento: eseguire un rapporto di tali account, esportarlo in Excel e quindi utilizzare la procedura guidata Importa lead dell'organizzazione per importare i dati come lead. Quindi, utilizzando l'eliminazione globale, selezionare "Account" come tipo di record da eliminare e specificare "Tipo uguale a Cliente potenziale" per individuare tutti gli account da eliminare.

- Si desidera eliminare tutti i lead che sono stati convertiti per la propria organizzazione. Selezionare il tipo di record lead, immettere "Convertito uguale a 1" come criterio di ricerca e quindi scegliere Cerca.
- Si desidera ripulire i lead generati dal Web che sono stati creati in modo non corretto, oppure eliminare account e referenti con i quali non si hanno più rapporti.

1. Si consiglia di eseguire un rapporto per archiviare le informazioni. Sarebbe inoltre opportuno eseguire un'esportazione settimanale dei propri dati; vedere Esportazione di dati di backup a pagina 437.
2. Da Imposta, immettere *Eliminazione globale record* nella casella `Ricerca veloce`, quindi selezionare **Eliminazione globale record** e fare clic sul link del tipo di record da eliminare.
3. Rivedere le informazioni che verranno eliminate con i record.

4. Specificare le condizioni che devono essere soddisfatte dagli elementi selezionati, ad esempio "Stato uguale California".
5. Se si eliminano gli account, specificare se si desidera eliminare gli account con opportunità chiuse/conseguite allegate o con opportunità allegate di cui sono titolari altri utenti.
6. Se si eliminano i prodotti, selezionare **Archiviare prodotti che hanno voci associate nelle opportunità** se si desidera eliminare anche i prodotti che si trovano nelle opportunità.

   Selezionare questa opzione per:

   - Eliminare i prodotti che non si trovano nelle opportunità e spostarli nel Cestino.
   - Archiviare i prodotti che si trovano nelle opportunità. Tali prodotti non vengono spostati nel Cestino e non possono essere recuperati.
7. Scegliere **Cerca** per trovare i record corrispondenti e selezionare gli elementi da eliminare. Se si desidera, selezionare la casella nell'intestazione di colonna per selezionare tutti i record correntemente visualizzati.
8. Per eliminare i record in modo permanente, selezionare `Eliminazione permanente dei record`.

   Importante: se si seleziona questa opzione non è più possibile ripristinare i record selezionati dal Cestino.
9. Fare clic su **Elimina**.

VEDERE ANCHE:

Note sull'utilizzo dell'eliminazione globale
Annullamento di un'importazione

# Note sull'utilizzo dell'eliminazione globale

Quando si utilizza l'eliminazione globale, prestare attenzione ai seguenti punti:

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **tutte** le versioni

Questa funzionalità è disponibile solo nella versione **Database.com Edition** mediante API. È possibile solo effettuare l'eliminazione globale dei record di oggetti personalizzati nella versione **Database.com Edition**.

AUTORIZZAZIONI UTENTE

Per eliminare globalmente dati:

- "Modifica tutti i dati"

## Note generali sull'eliminazione globale

- È possibile eliminare un massimo di 250 elementi alla volta.
- Quando si elimina un record, vengono eliminati anche i record associati visualizzati negli elenchi correlati del record specificato.
- È possibile procedere all'eliminazione globale unicamente dei rapporti presenti nelle cartelle rapporti pubbliche.
- Non è possibile effettuare l'eliminazione globale di record allegati a cruscotti digitali, pianificati o utilizzati nelle istantanee dei rapporti.

## Note sull'eliminazione globale per i team vendite

- Non è possibile eliminare account partner che possiedono utenti partner.
- Non è possibile eliminare, ma solo archiviare, i prodotti nelle opportunità.
- Quando si effettua l'eliminazione globale di prodotti, vengono eliminate anche tutte le relative voci del listino prezzi.
- Quando si eliminano attività, vengono eliminate anche tutte le attività archiviate che soddisfano le condizioni.

- Quando si eliminano attività, gli incontri richiesti non vengono inclusi nell'eliminazione globale finché non vengono confermati e automaticamente convertiti in eventi.
- Quando si eliminano eventi ricorrenti, i relativi eventi secondari non vengono visualizzati nell'elenco dei possibili elementi da eliminare, ma vengono eliminati.

## Note sull'eliminazione globale per i team di assistenza

- Non è possibile eliminare account e referenti associati a casi.
- Non è possibile eliminare i referenti abilitati per Self-Service e gli account associati.
- L'eliminazione di una soluzione principale non elimina le soluzioni tradotte associate. Ogni soluzione tradotta diventa invece una soluzione principale.
- L'eliminazione di una soluzione tradotta rimuove l'associazione alla relativa soluzione principale.

# Aggiornamento globale degli indirizzi

Quando i dati sono coerenti, i rapporti e le metriche correlate sono più precisi e facili da capire. Ad esempio, utilizzare abbreviazioni diverse per un paese può alterare i dati. Per rendere coerenti gli indirizzi, è possibile aggiornare una alla volta le informazioni relative a paese e provincia nei campi esistenti.

È possibile aggiornare globalmente gli indirizzi in referenti, contratti e lead.

Suggerimento: Per garantire la coerenza dei dati nei nuovi record, è consigliabile utilizzare gli elenchi di selezione provincia e paese.

1. Da Imposta, immettere `Aggiornamento globale indirizzi` nella casella `Ricerca veloce`, quindi selezionare **Aggiornamento globale indirizzi**.
2. Selezionare **Paesi** o **Stato/Provincia**. Se si sceglie Stato/Provincia, immettere il paese in cui si desidera aggiornare lo stato o la provincia.
3. Fare clic su **Avanti**.
4. Selezionare i valori da aggiornare e fare clic su **Aggiungi**. La casella Valori selezionati contiene i valori da aggiornare.

   Nella casella Valori disponibili vengono visualizzati i valori indirizzo trovati nei record esistenti. Per trovare altri indirizzi da aggiornare, immettere interamente o parzialmente il valore desiderato e fare clic su **Trova**.

   Se l'organizzazione dispone di una gran quantità di dati, invece di utilizzare la casella Valori disponibili, immettere i valori esistenti da aggiornare nell'area di testo. Separare ciascun valore con una nuova riga.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni tranne **Database.com** Edition

AUTORIZZAZIONI UTENTE

Per aggiornare globalmente gli indirizzi:
- "Modifica tutti i dati"

Per aggiornare globalmente gli indirizzi dei contratti:
- "Modifica tutti i dati"

  E

  "Attiva contratti"

5. Nel campo **Sostituisci valori selezionati con** immettere il valore con cui sostituire i dati indirizzo specificati e fare clic su **Avanti**. Se l'organizzazione dispone di una gran quantità di dati, il campo è denominato **Sostituisci valori immessi con**.

   Vengono visualizzati il numero e il tipo di record indirizzo da aggiornare. Se si utilizzano grandi quantità di dati, verranno visualizzati solo i valori da aggiornare.
6. Fare clic su **Sostituisci** per aggiornare i valori.

VEDERE ANCHE:

Elenchi di selezione Provincia e Paese

# Domande frequenti sulla scalabilità

- Quanto è scalabile Salesforce?
- Si verificano problemi di prestazioni con l'aumento della base di abbonati di Salesforce?

## Quanto è scalabile Salesforce?

Il servizio è in grado di adeguarsi anche ai team più numerosi. L'architettura su cui si basa è infatti stata progettata per gestire milioni di utenti. Possiamo adeguare la nostra capacità rapidamente in base alle richieste dei clienti.

## Si verificano problemi di prestazioni con l'aumento della base di abbonati di Salesforce?

No. Poiché siamo molto attenti alle prestazioni, il servizio è progettato per essere scalabile e permetterci così di anticipare costantemente le esigenze dei clienti. La nostra architettura ci consente di aggiungere facilmente server Web e di applicazioni per servire un maggior numero di utenti. L'architettura del sistema ci permette inoltre di aggiungere altri server di database in caso di aumento degli utenti. Inoltre, la struttura che ospita i nostri server ci garantisce una determinata larghezza di banda, che possiamo aumentare in funzione delle esigenze.

# Cache di Force.com Platform

# Definizione delle partizioni per i dati inseriti nella cache con la cache piattaforma di Force.com

EDIZIONI

Disponibile nelle versioni: **Enterprise Edition**, **Unlimited Edition**

Le partizioni consentono di ottimizzare le prestazioni distribuendo lo spazio della cache nel modo più appropriato per l'organizzazione. È possibile inserire i dati nelle partizioni designate nella cache per assicurarsi che non vengano sovrascritti da altre applicazioni o da dati di minore importanza. Le partizioni dell'organizzazione possono essere create e gestite in modo dichiarativo tramite lo strumento Partizione cache piattaforma in Imposta.

Le partizioni sono parte integrante dell'API e la funzionalità della cache dipende da esse. Per utilizzare la cache piattaforma di Force.com, è necessario disporre di almeno una partizione. Ogni partizione ha un segmento di cache sessione e uno di cache organizzazione. Ogni segmento di cache ha una propria capacità e propri attributi TTL (Time To Live) e utilizza un algoritmo LRU.

Utilizzare lo strumento Partizione cache piattaforma per:

- Creare o rimuovere le partizioni organizzazione.
- Assegnare la capacità della cache sessione e della cache organizzazione di ogni partizione in modo da bilanciare le prestazioni tra le applicazioni.
- Visualizzare un'istantanea di tutte le partizioni della cache con i valori della capacità corrente e della capacità totale.
- Visualizzare i dettagli relativi a ogni partizione.
- Impostare ogni partizione come partizione predefinita, ad esempio per utilizzarla tramite metodi statici.

Per prima cosa creare almeno una partizione e assegnare la capacità di cache ai segmenti di cache sessione e cache organizzazione della partizione. È possibile distribuire lo spazio della cache organizzazione nel numero desiderato di partizioni. Le assegnazioni di cache sessione e organizzazione possono essere zero o maggiori di cinque e devono essere numeri interi. La somma di tutte le assegnazioni

di partizioni, inclusa la partizione predefinita, è uguale all'assegnazione totale della cache piattaforma. La capacità totale assegnata di tutti i segmenti di cache deve essere uguale o inferiore alla capacità complessiva dell'organizzazione.

È possibile avere una sola partizione predefinita, ma si può definire qualsiasi partizione come partizione predefinita. Quando la capacità della partizione predefinita è stata tutta utilizzata ed è uguale a zero, non sarà possibile creare altre partizioni. Se una partizione non ha capacità residua, le operazioni di cache non vengono eseguite e non vengono restituiti errori.

Quando si eseguono operazioni nella cache all'interno della partizione predefinita, è possibile omettere il nome della partizione dalla chiave.

Nota: se il codice della cache piattaforma si riferisce a un pacchetto, si consiglia di non utilizzare la partizione predefinita nel pacchetto. Fare invece riferimento a una partizione non predefinita per il pacchetto.

Visualizzare l'assegnazione della capacità dell'organizzazione nella pagina Partizione cache piattaforma. Per accedere allo strumento Partizione in Imposta, immettere *Cache piattaforma* nella casella Ricerca veloce, quindi selezionare **Cache piattaforma**.

Per impostazione predefinita, i calcoli della capacità vengono eseguiti ogni cinque minuti. Per assicurarsi di visualizzare i valori più aggiornati di capacità e assegnazione, fare clic su **Ricalcola**.

VEDERE ANCHE:

*Force.com Apex Code Developer's Guide*

# Gestione dei record duplicati

## Gestione dei duplicati

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Gestire i propri dati in modo che siano sempre puliti e accurati è una delle cose più importanti se si desidera fare in modo che l'organizzazione utilizzi al meglio Salesforce. Utilizzare la funzione di gestione dei duplicati di Data.com per stabilire se e quando consentire agli utenti di creare record duplicati in Salesforce, personalizzare la logica utilizzata per identificare i duplicati e creare rapporti sui duplicati che vengono salvati dagli utenti.

Nota: la gestione dei duplicati utilizza la tecnologia Data.com ma *non* richiede una licenza Data.com.

Dopo aver impostato la gestione dei duplicati, attenersi alle istruzioni fornite di seguito.

- *Quando un utente tenta di salvare un nuovo record*, il record viene prima confrontato con i record Salesforce esistenti per identificare eventuali duplicati (1). I criteri utilizzati per confrontare i record e identificare i possibili duplicati vengono definiti da una *regola di corrispondenza*. Quindi, viene restituito un elenco di possibili duplicati (2). Ciò che accade quando il record salvato viene identificato come possibile duplicato dipende da ciò che è stato definito nella *regola di duplicazione* (3). Ad esempio, la regola di duplicazione può impedire agli utenti di salvare il possibile record duplicato o consentire comunque il salvataggio. Le opzioni Blocco e Consenti includono un avviso, che indica agli utenti il motivo per cui non possono salvare il record e ciò che devono fare. L'opzione Consenti include la possibilità di creare un rapporto sui record duplicati.

- *Quando un utente tenta di salvare un record modificato*, viene eseguito prima un controllo del record per verificare se l'utente ha modificato il valore di un campo di regola di corrispondenza. In caso affermativo, il processo di gestione dei duplicati esegue le operazioni descritte per i nuovi record. In caso negativo, non viene eseguita alcuna azione e i duplicati non vengono rilevati.

Per un elenco dei limiti, vedere Limiti della gestione dei duplicati.

VEDERE ANCHE:

Concetti di Gestione dei duplicati
Impostazione della Gestione dei duplicati in Salesforce
Riferimento per le regole di corrispondenza

# Concetti di Gestione dei duplicati

Per configurare più efficacemente la Gestione dei duplicati di Data.com, è importante comprendere alcuni concetti chiave.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

IN QUESTA SEZIONE:

Regole di duplicazione
Le regole di duplicazione vengono utilizzate per stabilire se e quando gli utenti possono salvare record duplicati in Salesforce.

Regole di corrispondenza
Le regole di corrispondenza vengono utilizzate per identificare i record duplicati in Salesforce.

Insiemi di record duplicati

È possibile visualizzare un elenco di record duplicati, raggruppati in insiemi duplicati, facendo clic sulla scheda Insiemi di record duplicati. Per eseguire questa operazione, l'organizzazione deve utilizzare l'azione rapporto con le relative regole di duplicazione.

Registri errori duplicati

Se l'organizzazione utilizza la Gestione dei duplicati Data.com, è possibile visualizzare qualsiasi errore di sistema che impedisca l'esecuzione delle regole di duplicazione o di corrispondenza.

Come la gestione della duplicazione influenza gli utenti

Quando sono state create e attivate le regole di duplicazione e gli utenti cercano di salvare un record che è stato identificato come un possibile duplicato, agli utenti verranno fornite indicazioni in merito a come procedere. Verrà visualizzato quanto segue.

## Regole di duplicazione

Le regole di duplicazione vengono utilizzate per stabilire se e quando gli utenti possono salvare record duplicati in Salesforce.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Le regole di duplicazione indicano a Salesforce quale azione intraprendere quando un utente tenta di creare un record duplicato. Ogni regola di duplicazione necessita di almeno una regola di corrispondenza per identificare quali record esistenti sono possibili duplicati.

È possibile configurare la regola di duplicazione in modo tale da eseguire un'azione quando viene creato un nuovo record e quando viene modificato un record già esistente. Tuttavia, la regola funzionerà per i record modificati solo se i campi da modificare sono inclusi nella regola di corrispondenza associata.

Esempio: La regola di duplicazione può impedire agli utenti di salvare i record che sono stati identificati come possibili duplicati oppure consentire loro di salvarli in ogni caso. Le opzioni Blocco e Consenti includono un avviso, che indica agli utenti il motivo per cui non possono salvare il record e ciò che devono fare. L'opzione Consenti include la possibilità di creare un rapporto sui record duplicati.

VEDERE ANCHE:

Creazione o modifica di regole di duplicazione

Gestione dei duplicati

## Regole di corrispondenza

Le regole di corrispondenza vengono utilizzate per identificare i record duplicati in Salesforce.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Guarda il video: Understanding Matching Rules (4:32)

Una regola di corrispondenza è costituita da singoli campi riuniti in un'equazione. Ogni campo contiene criteri di corrispondenza che indicano alla regola in che modo confrontare i campi e quali condizioni è necessario soddisfare affinché un campo specifico venga considerato una corrispondenza.

Dopo l'attivazione di una regola di corrispondenza, vengono automaticamente create una o più chiavi di corrispondenza da applicare ai record esistenti. Noto anche come indicizzazione, questo processo ottimizza le prestazioni e restituisce un gruppo di candidati più pertinenti per la corrispondenza poiché la regola cerca i duplicati solo tra i record che hanno la stessa chiave di corrispondenza.

Quando è attiva, la regola di corrispondenza confronta ogni campo con il campo corrispondente nei record esistenti che condividono le stesse chiavi di corrispondenza e utilizza i criteri di corrispondenza per determinare in che misura i campi, e quindi i record, corrispondono.

Esempio: Una regola di corrispondenza semplice può specificare che se i valori `Email` e `Telefono` di due record corrispondono esattamente, sono possibili duplicati. Oppure è possibile utilizzare diversi metodi di corrispondenza "fuzzy" per confrontare i campi.

Utilizzare le regole di corrispondenza con le regole di duplicazione per stabilire se e quando consentire agli utenti di creare record duplicati in Salesforce.

È possibile utilizzare le regole di corrispondenza standard o creare una propria regola di corrispondenza personalizzata. Si consiglia di utilizzare le regole di corrispondenza standard, in quanto sono state accuratamente ideate al fine di restituire il migliore insieme possibile di corrispondenze.

VEDERE ANCHE:

Creazione o modifica delle regole di corrispondenza personalizzate

Riferimento per le regole di corrispondenza

## Insiemi di record duplicati

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

È possibile visualizzare un elenco di record duplicati, raggruppati in insiemi duplicati, facendo clic sulla scheda Insiemi di record duplicati. Per eseguire questa operazione, l'organizzazione deve utilizzare l'azione rapporto con le relative regole di duplicazione.

Quando un utente salva un record identificato come duplicato da una regola di duplicazione mediante l'azione rapporto:

- Il record salvato e tutti i suoi duplicati, fino a un massimo di 100, verranno assegnati a un insieme di record duplicati nuovo o esistente.
- Il record salvato e ognuno dei suoi duplicati verranno elencati come elementi di record duplicati nell'insieme di record duplicati.
- Se la regola di duplicazione è configurata in modo da trovare i duplicati tra gli oggetti, tutti i duplicati rilevati verranno indicati come elementi di record duplicati nell'insieme di record duplicati.

Gli insiemi di record duplicati e gli elementi di record duplicati possono essere utilizzati per effettuare le operazioni indicate di seguito.

- Creare tipi di rapporto personalizzati
- Creare campi personalizzati
- Scrivere regole di convalida, trigger e regole di flusso di lavoro
- Modificare i campi che possono essere visualizzati sui rispettivi layout di pagina

Quando si utilizzano gli insiemi di record duplicati, tenere presenti alcuni fattori.

- Per impostazione predefinita, gli insiemi di record duplicati sono visibili solo agli amministratori, ma l'amministratore può concedere la visibilità agli altri utenti.
- Se un lead viene identificato come duplicato ma convertito prima che venga creato l'insieme di record duplicati, il lead convertito non verrà incluso in un insieme duplicato.

## Registri errori duplicati

Se l'organizzazione utilizza la Gestione dei duplicati Data.com, è possibile visualizzare qualsiasi errore di sistema che impedisca l'esecuzione delle regole di duplicazione o di corrispondenza.

Da Imposta, immettere *Registri errori duplicati* nella casella `Ricerca veloce`, quindi selezionare **Registri errori duplicati**. Da qui è possibile visualizzare gli eventuali errori che si sono verificati. I registri errori vengono eliminati dopo 90 giorni.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Esempio: Di seguito sono riportati alcuni scenari che potrebbero generare un errore sul registro.

- Il motore utilizzato per le corrispondenze "fuzzy" è temporaneamente indisponibile. Pertanto, le eventuali regole di corrispondenza che contengono metodi di corrispondenza "fuzzy" non verranno eseguite.
- L'azione Rapporto sulle regole di duplicazione non riesce in quanto il sistema non è in grado di creare un insieme di record duplicati.

## Come la gestione della duplicazione influenza gli utenti

Quando sono state create e attivate le regole di duplicazione e gli utenti cercano di salvare un record che è stato identificato come un possibile duplicato, agli utenti verranno fornite indicazioni in merito a come procedere. Verrà visualizzato quanto segue.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

- Tutte le regole di duplicazione includono un messaggio generato dal sistema (1) che indica all'utente il numero dei possibili duplicati rilevati. Il numero dei possibili duplicati comprende solo i record a cui l'utente ha accesso, anche se la protezione a livello di record della regola di duplicazione è stata impostata su `Ignora regole di condivisione`. L'opzione `Ignora regole di condivisione` indica alla regola di corrispondenza associata di confrontare tutti i record, indipendentemente dall'accesso dell'utente. Se l'utente non ha accesso a nessuno dei record identificati come possibili duplicati, questo messaggio indicherà solo la presenza di duplicati e il numero dei duplicati non viene incluso. I possibili duplicati visualizzati nell'elenco includono solo i record a cui è possibile accedere.
- Se la regola di duplicazione contiene un avviso, questo verrà visualizzato sotto il messaggio generato dal sistema (2).
- Se la regola di duplicazione consente agli utenti di salvare un record nonostante sia un possibile duplicato, sarà presente il pulsante **Salva (ignora avviso)** (3). Se la regola di duplicazione impedisce il salvataggio di un record che è un possibile duplicato, il pulsante **Salva** è presente ma il record non può essere salvato correttamente fino a che non vengono apportate al record le modifiche necessarie affinché non sia più contrassegnato come possibile duplicato.
- L'elenco dei possibili duplicati (4) include solo i record a cui è possibile accedere. I campi riportati nell'elenco includono solo i campi a cui l'utente ha accesso (al massimo i primi 7 campi confrontati dalla regola di corrispondenza associata). Nell'elenco appaiono al massimo 5 record, ma se vengono rilevati più di 5 duplicati, gli utenti possono fare clic su **Mostra tutto >>** per visualizzare l'elenco completo dei record (massimo 100). I record vengono elencati nell'ordine in cui sono stati modificati l'ultima volta. Gli utenti possono accedere direttamente a uno dei record dell'elenco, facendo clic sul relativo link.
- I campi evidenziati (5) sono i campi che sono stati confrontati dalla regola di corrispondenza associata e che sono risultati corrispondenti ai criteri.

VEDERE ANCHE:

Gestione dei duplicati

# Impostazione della Gestione dei duplicati in Salesforce

Per utilizzare la Gestione dei duplicati Data.com nell'organizzazione, sono necessarie due regole distinte: una regola di duplicazione e una regola di corrispondenza. La regola di duplicazione indica a Salesforce quale azione effettuare quando si identificano dei duplicati. La regola di corrispondenza definisce in che modo i record vengono confrontati gli uni con gli altri per identificare possibili duplicati.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

IN QUESTA SEZIONE:

Creazione o modifica di regole di duplicazione

Utilizzare le regole di duplicazione per definire cosa accade quando un utente cerca di salvare un record duplicato.

Creazione o modifica delle regole di corrispondenza personalizzate

Utilizzare le regole di corrispondenza per determinare in che modo due record vengono confrontati e identificati come duplicati.

Creazione di tipi di rapporto personalizzati per rapporti di record duplicati

Se l'organizzazione utilizza l'azione Rapporti con le relative regole di duplicazione, è possibile eseguire rapporti per analizzare la qualità dei dati e verificare il buon funzionamento delle regole di duplicazione. In questo modo è possibile perfezionare le regole di duplicazione, se necessario. Innanzitutto, è necessario impostare i tipi di rapporto personalizzati appropriati.

# Creazione o modifica di regole di duplicazione

Utilizzare le regole di duplicazione per definire cosa accade quando un utente cerca di salvare un record duplicato.

Per poter visualizzare l'elenco dei possibili duplicati rilevati dalla regola di duplicazione, gli utenti devono disporre di accesso in lettura all'oggetto definito nella regola.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare, modificare o eliminare le regole di duplicazione:
- "Personalizza applicazione"

Per attivare o disattivare le regole di duplicazione:
- “Personalizza applicazione”

Per visualizzare le regole di duplicazione:
- "Visualizza impostazione e configurazione"

1. Da Imposta, immettere *`Regole di duplicazione`* nella casella `Ricerca veloce` e selezionare **Regole di duplicazione**.
2. Per modificare una regola esistente, fare clic sul nome della regola e quindi su **Modifica**. Per creare una nuova regola, fare clic su **Nuova regola** e selezionare l'oggetto a cui si desidera applicarla.
3. Immettere i dettagli della regola, inclusi il nome, la descrizione e le impostazioni di protezione a livello di record.
4. Selezionare l'azione che si verificherà quando un utente cerca di salvare un record duplicato.

   Se l'azione include un avviso agli utenti, verrà fornito un testo di avviso predefinito che sarà possibile personalizzare. Solo l'azione Consenti include l'opzione del rapporto.
5. Nella sezione Regole di corrispondenza, selezionare prima l'oggetto con cui verranno confrontati i record. Quindi selezionare la regola di corrispondenza che determinerà il modo in cui i record verranno identificati come duplicati.

   L'elenco include tutte le regole di corrispondenza disponibili per l'oggetto selezionato. Se l'elenco non contiene la regola di corrispondenza desiderata, selezionare `Crea nuova regola di corrispondenza`.

   Suggerimento: Si consiglia di utilizzare le regole di corrispondenza standard, in quanto sono state accuratamente ideate al fine di restituire il migliore insieme possibile di corrispondenze. Verificare di averle attivate.

   Tuttavia, se si decide di creare una nuova regola di corrispondenza, consigliamo innanzitutto di terminare la creazione della regola di duplicazione. A questo punto creare e attivare la nuova regola di corrispondenza. Quando si torna alla regola di duplicazione, la medesima avrà automaticamente associata la regola di corrispondenza appena creata, a condizione che non avesse già una regola di corrispondenza associata.
6. Assicurarsi di avere selezionato la mappatura dei campi per ogni regola di corrispondenza, se necessario.

   Se la regola di corrispondenza confronta i record di due oggetti differenti o utilizza i campi personalizzati:
   - sarà necessario decidere in che modo i campi del primo oggetto dovranno essere confrontati con i campi del secondo oggetto. Ad esempio, è possibile mappare un campo personalizzato denominato `Email lavoro` al campo `Email` standard.
   - Alcuni dati possono essere troncati prima del confronto tra due campi con lunghezza massima diversa.
7. Se si desidera che la regola di duplicazione venga eseguita solo quando sono soddisfatte determinate condizioni, specificare tali condizioni.

   Ad esempio, si potrebbe aggiungere una condizione che prevede l'esecuzione della regola solo se il record è stato immesso da un utente con un determinato profilo o ruolo oppure se il record contiene un paese o una provincia specifici.
8. Salvare la regola.
9. Attivare la regola.

   Perché l'attivazione funzioni, è necessario che tutte le regole di corrispondenza associate siano attive.

10. Se per un determinato oggetto sono attive più regole di duplicazione, potrebbe essere utile modificare l'ordine in cui vengono elaborate. Per riordinare le regole, fare clic su **Riordina** dalla pagina dei dettagli di una delle regole.

    Suggerimento: Se la prima regola di duplicazione individua una corrispondenza per un record specifico, quel record non sarà valutato dalle regole di duplicazione successive. Pertanto, è opportuno ordinare le regole di duplicazione in modo che quelle con l'azione Blocco vengano eseguite prima di quelle con l'azione Consenti.

VEDERE ANCHE:

Regole di duplicazione
Regole di corrispondenza

## Creazione o modifica delle regole di corrispondenza personalizzate

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare, modificare o eliminare le regole di corrispondenza:
- "Personalizza applicazione"

Per attivare o disattivare le regole di corrispondenza:
- "Personalizza applicazione"

Per visualizzare le regole di corrispondenza:
- "Visualizza impostazione e configurazione"

Utilizzare le regole di corrispondenza per determinare in che modo due record vengono confrontati e identificati come duplicati.

1. Da Imposta, immettere `Regole di corrispondenza` nella casella `Ricerca veloce` e selezionare **Regole di corrispondenza**.
2. Se si modifica una regola di corrispondenza già esistente, assicurarsi che non sia attiva.
3. Fare clic su **Nuova regola** o su **Modifica** accanto alla regola esistente da modificare.
4. Selezionare l'oggetto a cui verrà applicata la regola di corrispondenza.
5. Assegnare un nome e una descrizione alla regola.
6. Immettere i criteri di corrispondenza.

   I criteri di corrispondenza consentono di definire i campi da confrontare e il metodo da utilizzare. Per aggiungere altri campi (fino a 10 in totale), fare clic su **Aggiungi logica dei filtri...** e quindi **Aggiungi riga**.
7. Se è necessario adeguare l'equazione di corrispondenza, fare clic su **Aggiungi logica dei filtri...**. Qui è possibile, ad esempio, modificare manualmente un'espressione AND in un'espressione OR.
8. Salvare la regola.
9. Attivare la regola.

   Il processo di attivazione può richiedere un certo tempo, quindi l'utente riceverà un'email al termine del processo e protrà iniziare a utilizzare la regola di corrispondenza.

Una volta attivata, la regola di corrispondenza è disponibile per l'uso con altri strumenti di gestione dei duplicati di Data.com. Ad esempio, l'utilizzo di una regola di corrispondenza con una regola di duplicazione indica a Salesforce di eseguire determinate operazioni quando l'utente tenta di salvare un record che la regola di corrispondenza ha identificato come duplicato.

VEDERE ANCHE:

Regole di corrispondenza
Riferimento per le regole di corrispondenza

## Creazione di tipi di rapporto personalizzati per rapporti di record duplicati

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per creare o aggiornare tipi di rapporto personalizzati:
- "Gestisci tipi di rapporto personalizzato"

Per eliminare i tipi di rapporto personalizzato:
- "Modifica tutti i dati"

Se l'organizzazione utilizza l'azione Rapporti con le relative regole di duplicazione, è possibile eseguire rapporti per analizzare la qualità dei dati e verificare il buon funzionamento delle regole di duplicazione. In questo modo è possibile perfezionare le regole di duplicazione, se necessario. Innanzitutto, è necessario impostare i tipi di rapporto personalizzati appropriati.

Gli unici record che verranno visualizzati in questi rapporti sono:

- I record identificati come duplicati dalle regole di duplicazione che includono l'azione del rapporto.
- I record che sono stati aggiunti manualmente all'oggetto Insieme di record duplicati.

1. Verificare di avere dimestichezza con i tipi di rapporto personalizzato e con il procedimento generale per la loro creazione e gestione.
2. Creare dei tipi di rapporto personalizzati con le relazioni tra oggetti appropriate e configurarli secondo necessità.

   Di seguito sono riportati alcuni esempi di tipi di rapporti personalizzati per iniziare.

| Tipo di rapporto | Utilizzo possibile | A (oggetto principale) | B | Fasi aggiuntive |
|---|---|---|---|---|
| Account duplicati | Creare rapporti sugli account duplicati che sono stati trovati dalle regole di duplicazione. | Account | Elementi di record duplicati | |
| Referenti duplicati | Creare rapporti sui referenti duplicati che sono stati trovati dalle regole di duplicazione. | Referenti | Elementi di record duplicati | |
| Lead duplicati | Creare rapporti sui lead duplicati che sono stati trovati dalle regole di duplicazione. | Lead | Elementi di record duplicati | |
| Tutti i duplicati | Creare rapporti per verificare il funzionamento delle regole di duplicazione. | Insieme di record duplicati | Elementi di record duplicati | Aggiungere il campo di ricerca `Nome regola di duplicazione` al layout di pagina Insieme di record duplicati. |

3. Distribuire i tipi di rapporto da mettere a disposizione degli utenti.
4. Comunicare agli utenti che possono creare rapporti utilizzando questi tipi di rapporto personalizzati.

VEDERE ANCHE:

Insiemi di record duplicati

# Riferimento per le regole di corrispondenza

Di seguito vengono fornite alcune informazioni aggiuntive sul funzionamento delle regole di corrispondenza e su come utilizzarle.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

IN QUESTA SEZIONE:

Regole di corrispondenza standard

Sono disponibili diverse regole di corrispondenza standard che l'utente può utilizzare con gli strumenti di gestione dei duplicati di Data.com, ad esempio le regole di duplicazione. Ogni regola di corrispondenza standard è stata progettata in modo da restituire il migliore insieme possibile di candidati per la corrispondenza di account, referenti o lead.

Criteri di corrispondenza per le regole di corrispondenza

Le regole di corrispondenza utilizzano dei criteri per determinare il livello di corrispondenza di un campo in un record nuovo o modificato con lo stesso campo in un record esistente e per stabilire se i due record corrispondono. Quando si crea una regola di corrispondenza personalizzata, è necessario definire determinati criteri. Le regole di corrispondenza standard includono criteri aggiuntivi che vengono definiti in modo specifico per l'utente.

Metodi di corrispondenza utilizzati con le regole di corrispondenza

Il metodo di corrispondenza è la parte dei criteri di una regola di corrispondenza he determina in che modo un campo specifico in un record viene confrontato con lo stesso campo in un altro record. Sono disponibili un metodo di corrispondenza esatta e una varietà di metodi di corrispondenza "fuzzy".

Algoritmi di corrispondenza utilizzati con i metodi di corrispondenza

Il metodo di corrispondenza e l'algoritmo di corrispondenza fanno parte dei criteri di una regola di corrispondenza. Insieme determinano in che modo un campo specifico in un record viene confrontato con lo stesso campo in un altro record e se i campi vengono considerati corrispondenze.

Chiavi di corrispondenza e regole di corrispondenza

Le chiavi di corrispondenza consentono di aumentare l'efficacia delle regole di corrispondenza. Comprendere in che modo vengono create le chiavi di corrispondenza consente di capire meglio il funzionamento delle regole di corrispondenza.

Chiavi di corrispondenza utilizzate dalle regole di corrispondenza standard

Le chiavi di corrispondenza consentono di aumentare l'efficacia delle regole di corrispondenza. Esaminare le informazioni sulle chiavi di corrispondenza per comprendere meglio il funzionamento delle regole di corrispondenza standard.

# Regole di corrispondenza standard

Sono disponibili diverse regole di corrispondenza standard che l'utente può utilizzare con gli strumenti di gestione dei duplicati di Data.com, ad esempio le regole di duplicazione. Ogni regola di corrispondenza standard è stata progettata in modo da restituire il migliore insieme possibile di candidati per la corrispondenza di account, referenti o lead.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

IN QUESTA SEZIONE:



## Regola di corrispondenza standard - Account

Come tutte le regole di corrispondenza, la regola di corrispondenza standard utilizzata per i record di account è composta da campi riuniti in un'equazione. Ogni campo contiene criteri di corrispondenza che la regola utilizza per determinare in che misura il campo corrisponde allo stesso campo in un record esistente e in definitiva se il record è una corrispondenza.

### Equazione di corrispondenza

Importante: Affinché la regola di corrispondenza standard per l'account restituisca le corrispondenze in modo preciso, il record nuovo o modificato deve includere un valore nel campo `Nome account` e nel campo `Città` o `CAP`.

| Nome regola | Equazione di corrispondenza |
|---|---|
| Regola di corrispondenza account standard | (*Nome account* AND *Indirizzo di fatturazione*)<br>OR (*Nome account* AND *Città*)<br>OR (*Nome account* AND *CAP*)<br>OR (*Nome account* AND *Telefono*)<br>OR (*Sito Web* AND *Telefono*)<br>OR (*Sito Web* AND *Indirizzo di fatturazione*) |

### Criteri di corrispondenza

Per una definizione di ogni criterio di corrispondenza, vedere Criteri di corrispondenza per le regole di corrispondenza a pagina 464.

| Campo | Algoritmi di corrispondenza | Metodo di assegnazione del punteggio | Soglia | Campi vuoti | Gestione speciale |
|---|---|---|---|---|---|
| `Nome account` | Acronimo<br>Distanza di modifica<br>Esatta | Massimo | 70 | Non corrispondono | Rimuove parole come `Inc` e `Corp` prima di confrontare i campi. Inoltre, i nomi delle società vengono normalizzati. Ad esempio, `1st National Bank` viene normalizzato in `First National Bank`. |
| `Telefono` | Esatta | Media ponderata | 80 | Non corrispondono in tutte le sezioni tranne quella del prefisso, che ignora i campi vuoti | I numeri di telefono vengono suddivisi in sezioni e confrontati in base alle sezioni. Ogni sezione ha un metodo e un punteggio di corrispondenza propri. I punteggi delle sezioni vengono ponderati in modo da fornire un solo punteggio per il campo. Questo processo funziona in modo ottimale con i dati relativi al Nord America.<br>• Codice internazionale (Esatta, 10% di punteggio di corrispondenza del campo)<br>• Prefisso (Esatta, 50% di punteggio di corrispondenza del campo)<br>• 3 cifre successive (Esatta, 30% di punteggio di corrispondenza del campo)<br>• Ultime 4 cifre (Esatta, 10% di punteggio di corrispondenza del campo)<br>Ad esempio, si supponga di confrontare questi due numeri di telefono: *`1-415-555-1234`* e *`1-415-555-5678`*.<br>Tutte le sezioni corrispondono esattamente *tranne* le ultime 4 cifre, quindi il punteggio di corrispondenza del campo è 90, valore che viene considerato come corrispondenza poiché supera la soglia di 80. |
| `Via fatturazione` | Distanza di modifica<br>Esatta | Media ponderata | 80 | Non corrispondono | Gli indirizzi vengono suddivisi in sezioni e confrontati in base alle sezioni. Ogni sezione ha un metodo e un punteggio di corrispondenza propri. I punteggi delle sezioni vengono ponderati in modo da fornire un solo punteggio per il campo. Questo processo funziona in modo ottimale con i dati relativi al Nord America.<br>• Numero (Esatta, 20% di punteggio di corrispondenza del campo)<br>• Via (Distanza di modifica, 50% di punteggio di corrispondenza del campo)<br>• Suffisso via (Esatta, 15% di punteggio di corrispondenza del campo)<br>• Numero suite (Esatta, 15% di punteggio di corrispondenza del campo) |

| Campo | Algoritmi di corrispondenza | Metodo di assegnazione del punteggio | Soglia | Campi vuoti | Gestione speciale |
|---|---|---|---|---|---|
| | | | | | Ad esempio, si supponga di confrontare questi due indirizzi di fatturazione: *123 Market Street, Suite 100* e *123 Market Drive, Suite 300*.<br>Poiché corrispondono solo la via e il numero, il punteggio di corrispondenza del campo è 70, valore che non viene considerato come corrispondenza perché è inferiore alla soglia di 80. |
| CAP | Esatta | Media ponderata | 80 | Non corrispondono | I codici postali vengono suddivisi in sezioni e confrontati in base alle sezioni. Ogni sezione ha un metodo e un punteggio di corrispondenza propri. I punteggi delle sezioni vengono ponderati in modo da fornire un solo punteggio per il campo.<br>• Prime 5 cifre (Esatta, 90% di punteggio di corrispondenza del campo)<br>• 4 cifre successive (Esatta, 10% di punteggio di corrispondenza del campo)<br>Ad esempio, si supponga di confrontare questi due CAP: *94104-1001* e *94104*.<br>Poiché corrispondono solo le prime 5 cifre, il punteggio di corrispondenza del campo è 90, valore che viene considerato come corrispondenza poiché supera la soglia di 80. |
| Città | Distanza di modifica<br>Esatta | Massimo | 85 | Non corrispondono | |
| Sito Web | Esatta | Massimo | 100 | Non corrispondono | Viene confrontato solo il dominio del sito Web. Ad esempio, il valore di campo `http://www.salesforce.com` diventa `salesforce.com`. |

VEDERE ANCHE:

Riferimento per le regole di corrispondenza

## Regola di corrispondenza standard - Referenti e lead

Come tutte le regole di corrispondenza, la regola di corrispondenza standard utilizzata per i record di referenti e lead è composta da campi riuniti in un'equazione. Ogni campo contiene inoltre criteri di corrispondenza che la regola utilizza per determinare in che misura il campo corrisponde allo stesso campo in un record esistente e in definitiva se il record è una corrispondenza.

## Equazione di corrispondenza

| Nome regola | Equazione di corrispondenza |
|---|---|
| Regola di corrispondenza referente standard<br>Regola di corrispondenza lead standard | (*Nome* AND *Cognome* AND *Qualifica* AND *Nome azienda*)<br>OR (*Nome* AND *Cognome* AND *Email*)<br>OR (*Nome* AND *Cognome* AND *Telefono* AND *Nome azienda*)<br>OR (*Nome* AND *Cognome* AND *Indirizzo postale* AND (*Città* OR *CAP* OR *Telefono*)<br>OR (*Nome* AND *Cognome* AND *Indirizzo postale* AND *Qualifica*)<br>OR (*Nome* AND *Cognome* AND *Qualifica* AND *Email*)<br>OR (*Nome* AND *Cognome* AND *Telefono*) |

## Criteri di corrispondenza

Per una definizione di ogni criterio di corrispondenza, vedere Criteri di corrispondenza per le regole di corrispondenza a pagina 464.

| Campi per referenti | Campi per lead | Algoritmi di corrispondenza | Metodo di assegnazione del punteggio | Soglia | Campi vuoti | Gestione speciale |
|---|---|---|---|---|---|---|
| Nome | Nome | Esatta<br>Iniziali<br>Distanza di Jaro-Winkler<br>Metaphone 3<br>Variante nome | Massimo | 85 | Non corrispondono (ignora i campi vuoti quando viene incluso Email nel gruppo di campi) | Se il record contiene un valore per entrambi i campi `Nome` e `Cognome`, tali valori verranno invertiti per verificare se vi sono errori di immissione dei dati.<br>Ad esempio, se il nome è *George* e il cognome è *Michael*, la regola di corrispondenza valuterà *Michael* anche come nome e *George* come cognome. |
| Cognome | Cognome | Esatta<br>Distanza tastiera<br>Metaphone 3 | Massimo | 90 | Non corrispondono (ignora i campi vuoti quando viene incluso Email nel gruppo di campi) | Se il record contiene un valore per entrambi i campi `Nome` e `Cognome`, tali valori verranno invertiti per verificare se vi sono errori di immissione dei dati.<br>Ad esempio, se il nome è *George* e il cognome è *Michael*, la regola di corrispondenza valuterà *Michael* anche come nome e *George* come cognome. |
| Qualifica | Qualifica | Acronimo<br>Esatta | Massimo | 50 | Non corrispondono | |

| Campi per referenti | Campi per lead | Algoritmi di corrispondenza | Metodo di assegnazione del punteggio | Soglia | Campi vuoti | Gestione speciale |
|---|---|---|---|---|---|---|
| | | Distanza di Kullback-Liebler | | | | |
| Nome account | Società | Acronimo<br>Distanza di modifica<br>Esatta | Massimo | 70 | Non corrispondono | |
| Email | Email | Esatta | Massimo | 100 | Non corrispondono | |
| Telefono | Telefono | Esatta | Media ponderata | 80 | Non corrispondono in tutte le sezioni tranne quella del prefisso, che ignora i campi vuoti | I numeri di telefono vengono suddivisi in sezioni e confrontati in base alle sezioni. Ogni sezione ha un metodo e un punteggio di corrispondenza propri. I punteggi delle sezioni vengono ponderati in modo da fornire un solo punteggio per il campo. Questo processo funziona in modo ottimale con i dati relativi al Nord America.<br>• Codice internazionale (Esatta, 10% di punteggio di corrispondenza del campo)<br>• Prefisso (Esatta, 50% di punteggio di corrispondenza del campo)<br>• 3 cifre successive (Esatta, 30% di punteggio di corrispondenza del campo)<br>• Ultime 4 cifre (Esatta, 10% di punteggio di corrispondenza del campo)<br>Ad esempio, si supponga di confrontare questi due numeri di telefono: `1-415-555-1234` e `1-415-555-5678`.<br>Tutte le sezioni corrispondono esattamente *tranne* le ultime 4 cifre, quindi il punteggio di corrispondenza del campo è 90, valore che viene considerato come corrispondenza poiché supera la soglia di 80. |
| Indirizzo postale | Via | Esatta | Media ponderata | 80 | Non corrispondono | Gli indirizzi vengono suddivisi in sezioni e confrontati in base alle sezioni. Ogni sezione ha un metodo e un punteggio di corrispondenza propri. I punteggi delle sezioni vengono ponderati in modo da fornire un solo punteggio per il campo. Questo processo funziona in modo ottimale con i dati relativi al Nord America. |

| Campi per referenti | Campi per lead | Algoritmi di corrispondenza | Metodo di assegnazione del punteggio | Soglia | Campi vuoti | Gestione speciale |
|---|---|---|---|---|---|---|
| | | | | | | • Via (Distanza di modifica, 50% di punteggio di corrispondenza del campo)<br>• Numero (Esatta, 20% di punteggio di corrispondenza del campo)<br>• Suffisso via (Esatta, 15% di punteggio di corrispondenza del campo)<br>• Numero suite (Esatta, 15% di punteggio di corrispondenza del campo)<br>Ad esempio, si supponga di confrontare questi due indirizzi: *123 Market Street, Suite 100* e *123 Market Drive, Suite 300*.<br>Poiché corrispondono solo la via e il numero, il punteggio di corrispondenza del campo è 70, valore che non viene considerato come corrispondenza perché è inferiore alla soglia di 80. |
| CAP/Codice postale | CAP/Codice postale | Esatta | Media ponderata | 80 | | I codici postali vengono suddivisi in sezioni e confrontati in base alle sezioni. Ogni sezione ha un metodo e un punteggio di corrispondenza propri. I punteggi delle sezioni vengono ponderati in modo da fornire un solo punteggio per il campo.<br>• Prime 5 cifre (Esatta, 90% di punteggio di corrispondenza del campo)<br>• 4 cifre successive (Esatta, 10% di punteggio di corrispondenza del campo) |
| Città indirizzo postale | Città | Distanza di modifica<br>Esatta | Massimo | 85 | Non corrispondono | |

VEDERE ANCHE:

Riferimento per le regole di corrispondenza

## Criteri di corrispondenza per le regole di corrispondenza

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Le regole di corrispondenza utilizzano dei criteri per determinare il livello di corrispondenza di un campo in un record nuovo o modificato con lo stesso campo in un record esistente e per stabilire se i due record corrispondono. Quando si crea una regola di corrispondenza personalizzata, è necessario definire determinati criteri. Le regole di corrispondenza standard includono criteri aggiuntivi che vengono definiti in modo specifico per l'utente.

Nota: Questo rilascio contiene una versione beta della funzionalità di gestione dei duplicati di Data.com, con una qualità pari all'istanza di produzione ma con limitazioni note. È possibile inviare commenti e suggerimenti sulla Comunità di successo Salesforce. Per informazioni sull'abilitazione di questa funzione per la propria organizzazione, contattare Salesforce.

| Criterio | Definizione | Definito automaticamente per le regole di corrispondenza personalizzate |
| --- | --- | --- |
| Campo | Indica quale campo confrontare. Quando si selezionano i campi, tenere presente quanto segue:<br>• I campi disponibili dipendono dall'oggetto a cui viene applicata la regola di corrispondenza e includono campi sia standard che personalizzati.<br>• I tipi di campi di input supportati sono email, relazione di ricerca, numero, telefono, elenco di selezione standard, elenco di selezione personalizzato (solo a selezione singola), testo e URL.<br>• Un campo di relazione di ricerca con numerazione automatica non può essere utilizzato in una regola di corrispondenza.<br>• Se si abilitano gli elenchi di selezione `Stato` e `Paese` per l'organizzazione, è consigliabile utilizzare **Codice stato/provincia** e **Codice paese** nelle regole di corrispondenza. Questi campi producono migliori risultati di rilevamento dei duplicati rispetto ai campi di testo stato e paese. | |
| Metodo di corrispondenza | Definisce il modo in cui i campi vengono confrontati. Sono disponibili un metodo di corrispondenza esatta e diversi metodi di corrispondenza "fuzzy". Ogni metodo di corrispondenza viene ulteriormente definito mediante algoritmi di corrispondenza e altri criteri.<br>Per ulteriori informazioni sui metodi di corrispondenza, vedere Metodi di corrispondenza utilizzati con le regole di corrispondenza a pagina 467. | |
| Algoritmo di corrispondenza | Definisce la logica che determina se 2 campi corrispondono. Per il metodo di corrispondenza esatta viene automaticamente utilizzato l'algoritmo di corrispondenza esatta. Per il metodo di corrispondenza "fuzzy" possono essere utilizzati diversi algoritmi di corrispondenza "fuzzy". A ogni algoritmo di corrispondenza utilizzato viene | ✓ |

| Criterio | Definizione | Definito automaticamente per le regole di corrispondenza personalizzate |
| --- | --- | --- |
| | automaticamente assegnato un punteggio che indica il livello di corrispondenza tra due campi che l'algoritmo è in grado di fornire. Ad esempio, se si seleziona la corrispondenza esatta e i due campi corrispondono, il punteggio di corrispondenza è 100, se i 2 campi non corrispondono, il punteggio è 0.<br>Per ulteriori informazioni sugli algoritmi di corrispondenza, vedere Algoritmi di corrispondenza utilizzati con i metodi di corrispondenza a pagina 470. | |
| Corrispondenza campi vuoti | Specifica se nel caso in cui 2 campi confrontati siano vuoti, i campi debbano essere considerati corrispondenze. Se si seleziona la casella di controllo `Corrispondenza campi vuoti` per un campo e il campo è vuoto in *entrambi* i record confrontati, i campi vengono considerati corrispondenze. Se tuttavia si seleziona la casella di controllo `Corrispondenza campi vuoti` per un campo e quel campo è vuoto *solo in uno* dei record confrontati, i campi non vengono considerati corrispondenze.<br>Se non si seleziona la casella di controllo `Corrispondenza campi vuoti` per un campo e quel campo è vuoto in *entrambi* i record confrontati, i campi *non* verranno considerati corrispondenze. | |
| Metodo di assegnazione del punteggio | Determina il modo in cui vengono calcolati i punteggi degli algoritmi di corrispondenza per assegnare un unico punteggio a un campo. A ogni algoritmo di corrispondenza utilizzato viene automaticamente assegnato un punteggio basato sul livello di corrispondenza ottenuto per due campi confrontati. Il metodo di assegnazione del punteggio viene utilizzato solo dalle regole di corrispondenza standard.<br>*`Media`*: utilizza il punteggio di corrispondenza medio.<br>*`Massimo`*: utilizza il punteggio di corrispondenza più alto.<br>*`Minimo:`* utilizza il punteggio di corrispondenza più basso.<br>*`Media ponderata`*: utilizza il valore ponderato di ogni metodo di corrispondenza per determinare il punteggio medio della corrispondenza. | ✓ |
| Soglia | Determina il punteggio di corrispondenza minimo necessario per considerare il campo una corrispondenza. Al campo viene automaticamente assegnato un punteggio di corrispondenza basato sul livello di corrispondenza dello stesso campo in un record esistente. | ✓ |
| Chiave di corrispondenza | Codice che consente alla regola di corrispondenza di restituire rapidamente un elenco di possibili duplicati. Una volta attivata la regola di corrispondenza, il codice viene automaticamente applicato a tutti i record esistenti in modo tale che quando viene eseguita, la regola di corrispondenza cerchi i duplicati solo tra i record con la stessa chiave di corrispondenza. Questo processo ottimizza le prestazioni e restituisce un insieme di candidati più pertinenti per la corrispondenza.<br>Per ulteriori informazioni sulle chiavi di corrispondenza, inclusi i relativi esempi, vedere Chiavi di corrispondenza e regole di corrispondenza a pagina 471. | ✓ |

## Esempio

Esempio: Applicando una regola di corrispondenza personalizzata per i referenti che include i seguenti criteri, il confronto e la corrispondenza tra i record vengono eseguiti come segue.

- L'equazione di corrispondenza è `Email` AND (`Phone` OR `City`).
- Tutti i campi utilizzano il metodo di corrispondenza esatta.
- Viene selezionata la casella di controllo `Corrispondenza campi vuoti` per `Phone` e `City`.

**Nuovo record A**

| Email | Telefono | Città |
| --- | --- | --- |
| jdoe@salesforce.com | 415-555-1234 | San Francisco |

**Record esistenti confrontati con il nuovo record A**

| Record | Email | Punteggio corrispondenza email | Telefono | Punteggio corrispondenza telefono | Città | Punteggio corrispondenza città | Il record corrisponde? |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | jdoe@salesforce.com | 100 | 415-555-1234 | 100 | nessuno | 0 | Sì |
| 2 | jdoe@salesforce.com | 100 | nessuno | 0 | San Francisco | 100 | Sì |
| 3 | jsmith@salesforce.com | 0 | 415-555-1234 | 100 | San Francisco | 100 | No |
| 4 | nessuno | 0 | 415-555-1234 | 100 | Oakland | 0 | No |
| 5 | jdoe@salesforce.com | 100 | 415–555-7777 | 0 | San Jose | 0 | No |

**Nuovo record B**

| Email | Telefono | Città |
| --- | --- | --- |
| jdoe@salesforce.com | nessuno | nessuno |

**Record esistenti confrontati con il nuovo record B**

| Record | Email | Punteggio corrispondenza email | Telefono | Punteggio corrispondenza telefono | Città | Punteggio corrispondenza città | Il record corrisponde? |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | jdoe@salesforce.com | 100 | 415-555-1234 | 0 | nessuno | 100 | Sì |
| 2 | jdoe@salesforce.com | 100 | nessuno | 100 | San Francisco | 0 | Sì |
| 3 | jdoe@salesforce.com | 100 | nessuno | 100 | nessuno | 100 | Sì |
| 4 | jsmith@salesforce.com | 0 | 415-555-1234 | 0 | San Francisco | 0 | No |

| Record | Email | Punteggio corrispondenza email | Telefono | Punteggio corrispondenza telefono | Città | Punteggio corrispondenza città | Il record corrisponde? |
|---|---|---|---|---|---|---|---|
| 5 | nessuno | 0 | 415-555-1234 | 0 | Oakland | 0 | No |

VEDERE ANCHE:

Riferimento per le regole di corrispondenza

## Metodi di corrispondenza utilizzati con le regole di corrispondenza

Il metodo di corrispondenza è la parte dei criteri di una regola di corrispondenza he determina in che modo un campo specifico in un record viene confrontato con lo stesso campo in un altro record. Sono disponibili un metodo di corrispondenza esatta e una varietà di metodi di corrispondenza "fuzzy".

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

| Metodo di corrispondenza | Descrizione |
|---|---|
| Esatta | Questo metodo cerca le stringhe che corrispondono esattamente a uno schema. Se si utilizzano dati internazionali, si consiglia di utilizzare il metodo di corrispondenza esatta con le regole di corrispondenza. |
| Fuzzy | Questo metodo cerca le stringhe che corrispondono a uno schema con una certa approssimazione. È disponibile la logica per una varietà di metodi di corrispondenza "fuzzy". |

Per una definizione di ogni criterio di corrispondenza, vedere Criteri di corrispondenza per le regole di corrispondenza a pagina 464.

| Metodo di corrispondenza fuzzy | Algoritmi di corrispondenza | Metodo di assegnazione del punteggio | Soglia | Gestione speciale |
|---|---|---|---|---|
| Fuzzy: Nome | Esatta<br>Iniziali<br>Jaro-Winkler<br>Variante nome | Massimo | 85 | Il campo `Secondo nome`, se utilizzato nella regola di corrispondenza, viene confrontato dal metodo di corrispondenza Fuzzy: Nome. |
| Fuzzy: Cognome | Esatta<br>Distanza tastiera<br>Metaphone 3 | Massimo | 90 | |

| Metodo di corrispondenza fuzzy | Algoritmi di corrispondenza | Metodo di assegnazione del punteggio | Soglia | Gestione speciale |
|---|---|---|---|---|
| Fuzzy: Nome società | Acronimo<br>Esatta<br>Allineamento sillabe | Massimo | 70 | Rimuove parole come `Inc` e `Corp` prima di confrontare i campi. Inoltre, i nomi delle società vengono normalizzati. Ad esempio, `IBM` viene normalizzato in `International Business Machines`. |
| Fuzzy: Telefono | Esatta | Media ponderata | 80 | I numeri di telefono vengono suddivisi in sezioni e confrontati in base alle sezioni. Ogni sezione ha un metodo e un punteggio di corrispondenza propri. I punteggi delle sezioni vengono ponderati in modo da fornire un solo punteggio per il campo. Questo processo funziona in modo ottimale con i dati relativi al Nord America.<br>• Codice internazionale (Esatta, 10% di punteggio di corrispondenza del campo)<br>• Prefisso (Esatta, 50% di punteggio di corrispondenza del campo)<br>• 3 cifre successive (Esatta, 30% di punteggio di corrispondenza del campo)<br>• Ultime 4 cifre (Esatta, 10% di punteggio di corrispondenza del campo)<br>Ad esempio, si supponga di confrontare questi due numeri di telefono: *`1-415-555-1234`* e *`1-415-555-5678`*.<br>Tutte le sezioni corrispondono esattamente *tranne* le ultime 4 cifre, quindi il punteggio di corrispondenza del campo è 90, valore che viene considerato come corrispondenza poiché supera la soglia di 80. |
| Fuzzy: Città | Distanza di modifica<br>Esatta | Massimo | 85 | |
| Fuzzy: Via | Esatta | Media ponderata | 80 | Gli indirizzi vengono suddivisi in sezioni e confrontati in base alle sezioni. Ogni sezione ha un metodo e un punteggio di corrispondenza propri. I punteggi delle sezioni vengono ponderati in modo da fornire un solo punteggio per il campo. Questo processo funziona in modo ottimale con i dati relativi al Nord America.<br>• Via (Distanza di modifica, 50% di punteggio di corrispondenza del campo) |

| Metodo di corrispondenza fuzzy | Algoritmi di corrispondenza | Metodo di assegnazione del punteggio | Soglia | Gestione speciale |
| --- | --- | --- | --- | --- |
| | | | | • Numero (Esatta, 20% di punteggio di corrispondenza del campo)<br>• Suffisso via (Esatta, 15% di punteggio di corrispondenza del campo)<br>• Numero suite (Esatta, 15% di punteggio di corrispondenza del campo)<br>Ad esempio, si supponga di confrontare questi due indirizzi di fatturazione: `123 Market Street, Suite 100` e `123 Market Drive, Suite 300`.<br>Poiché corrispondono solo la via e il numero, il punteggio di corrispondenza del campo è 70, valore che non viene considerato come corrispondenza perché è inferiore alla soglia di 80. |
| Fuzzy: CAP | Esatta | Media ponderata | 80 | I codici postali vengono suddivisi in sezioni e confrontati in base alle sezioni. Ogni sezione ha un metodo e un punteggio di corrispondenza propri. I punteggi delle sezioni vengono ponderati in modo da fornire un solo punteggio per il campo.<br>• Prime 5 cifre (Esatta, 90% di punteggio di corrispondenza del campo)<br>• 4 cifre successive (Esatta, 10% di punteggio di corrispondenza del campo)<br>Ad esempio, si supponga di confrontare questi due CAP: `94104-1001` e `94104`.<br>Poiché corrispondono solo le prime 5 cifre, il punteggio di corrispondenza del campo è 90, valore che viene considerato come corrispondenza poiché supera la soglia di 80. |
| Fuzzy: Titolo | Acronimo<br>Esatta<br>Distanza di Kullback-Liebler | Massimo | 50 | |

# Algoritmi di corrispondenza utilizzati con i metodi di corrispondenza

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Il metodo di corrispondenza e l'algoritmo di corrispondenza fanno parte dei criteri di una regola di corrispondenza. Insieme determinano in che modo un campo specifico in un record viene confrontato con lo stesso campo in un altro record e se i campi vengono considerati corrispondenze.

Sono disponibili un metodo di corrispondenza esatta e una varietà di metodi di corrispondenza "fuzzy". Se viene selezionato il metodo di corrispondenza esatta, per confrontare i campi viene automaticamente utilizzato l'algoritmo di corrispondenza esatta Se si seleziona uno dei metodi di corrispondenza "fuzzy", verrà utilizzata una varietà di algoritmi di corrispondenza "fuzzy" per confrontare i campi. Un campo può essere confrontato utilizzando più di un algoritmo di corrispondenza e viene assegnato un punteggio di corrispondenza a ogni algoritmo in base al livello di corrispondenza tra i campi che è in grado di fornire. I campi confrontati con gli algoritmi di corrispondenza *non* fanno distinzione tra maiuscole e minuscole.

Per ulteriori informazioni sui metodi di corrispondenza, vedere Metodi di corrispondenza utilizzati con le regole di corrispondenza a pagina 467.

**Algoritmi di corrispondenza disponibili con il metodo di corrispondenza esatta**

| Algoritmo di corrispondenza | Descrizione |
| --- | --- |
| Esatta | Determina se due stringhe corrispondono. Ad esempio, salesforce.com e Salesforce non sono considerati una corrispondenza perché non coincidono esattamente e viene restituito un punteggio pari a 0. |

**Algoritmi di corrispondenza disponibili con il metodo di corrispondenza "fuzzy"**

| Algoritmo di corrispondenza | Descrizione |
| --- | --- |
| Acronimo | Determina se un nome aziendale corrisponde al relativo acronimo. Ad esempio, Advanced Micro Devices e l'acronimo AMD sono considerati una corrispondenza e restituiscono 100 come punteggio di corrispondenza. |
| Distanza di modifica | Determina la similarità tra due stringhe in base al numero di eliminazioni, inserimenti e sostituzioni di caratteri necessari per trasformare una stringa nell'altra. Ad esempio, "VP Sales" corrisponde a "VP of Sales" con punteggio di corrispondenza 73. |
| Iniziali | Determina la similarità di due gruppi di iniziali nei nomi di persona. Ad esempio, il nome Jonathan e la sua iniziale J corrispondono e restituiscono il punteggio di corrispondenza 100. |
| Distanza di Jaro-Winkler | Determina la similarità tra due stringhe in base al numero di sostituzioni di caratteri necessari per trasformare una stringa nell'altra. Questo metodo è ideale per le stringhe brevi, come i nomi di persona. Ad esempio, Johnny corrisponde a Johny con punteggio di corrispondenza 97. |
| Distanza tastiera | Determina la similarità tra due stringhe in base al numero di eliminazioni, inserimenti e sostituzioni di caratteri necessari per trasformare una stringa nell'altra, misurata in base alla posizione dei tasti sulla tastiera. |

| Algoritmo di corrispondenza | Descrizione |
|---|---|
| Distanza di Kullback-Liebler | Determina la similarità tra due stringhe in base alla percentuale di parole in comune. Ad esempio, "Director of Engineering" corrisponde a "Engineering Director" con punteggio di corrispondenza 65. |
| Metaphone 3 | Determina la similarità tra due stringhe in base al suono che producono. Questo algoritmo tenta di rappresentare le irregolarità tra le lingue e funziona bene per i nomi e i cognomi. Ad esempio, Joseph corrisponde a Josef con punteggio di corrispondenza 100. |
| Variante nome | Determina se due nomi sono variazioni l'uno dell'altro. Ad esempio, Bob è una variazione di Robert e restituisce un punteggio di corrispondenza pari a 100. Bob non è una variazione di Bill e restituisce il punteggio 0. |

VEDERE ANCHE:

Riferimento per le regole di corrispondenza

## Chiavi di corrispondenza e regole di corrispondenza

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Le chiavi di corrispondenza consentono di aumentare l'efficacia delle regole di corrispondenza. Comprendere in che modo vengono create le chiavi di corrispondenza consente di capire meglio il funzionamento delle regole di corrispondenza.

Una *chiave di corrispondenza* è un codice che consente a una regola di corrispondenza di restituire rapidamente un elenco di possibili duplicati. Una volta attivata la regola di corrispondenza, il codice viene automaticamente applicato a tutti i record esistenti in modo tale che quando viene eseguita, la regola di corrispondenza cerchi i duplicati solo tra i record con la stessa chiave di corrispondenza. Questo processo, noto anche come indicizzazione, ottimizza le prestazioni e restituisce un insieme di candidati più pertinenti per la corrispondenza.

Le chiavi di corrispondenza per le regole di corrispondenza standard e personalizzate vengono create automaticamente in base ai campi presenti nella regola di corrispondenza. Poiché ogni regola di corrispondenza personalizzata può avere solo 10 chiavi di corrispondenza, l'utente non avrà la possibilità di salvare una regola di corrispondenza che richiede più di 10 chiavi di corrispondenza.

Il processo di creazione delle chiavi di corrispondenza prevede diversi passaggi.

1. L'equazione della regola di corrispondenza (ovvero la disposizione dei campi) viene riscritta in un formato standardizzato che traduce le istruzioni OR in istruzioni AND.
2. I campi vengono normalizzati utilizzando gli stessi metodi delle regole di corrispondenza standard. Per informazioni, vedere Chiavi di corrispondenza utilizzate dalle regole di corrispondenza standard a pagina 472.
3. Il formato di campo standardizzato e i valori di campo normalizzati vengono combinati per creare le chiavi di corrispondenza.

Nota: Attualmente non vengono create chiavi di corrispondenza per i campi `Titolo` e `Indirizzo`. Di conseguenza, se tali campi vengono inclusi nella regola di corrispondenza, non generano chiavi di corrispondenza.

Esempio: **Esempio**

| Nome campo | Valore campo | Valore campo normalizzato |
|---|---|---|
| Nome | John | j |

| Nome campo | Valore campo | Valore campo normalizzato |
| --- | --- | --- |
| Email | john_oreilly@us.intel.com | joreilly@intelcom |
| Cognome | O'Reilly | arl |
| Società | Intel Corp. | intel |

| Equazione regola di corrispondenza | Formato standardizzato | Chiavi di corrispondenza (combinazioni di campi) | Chiavi di corrispondenza (con valori di campo normalizzati) |
| --- | --- | --- | --- |
| (Nome OR Email) AND (Cognome OR Società) | (Nome AND Cognome) OR | Nome Cognome | jarl |
| | (Nome AND Società) OR | Nome Società | jintel |
| | (Email AND Cognome) OR | Email Cognome | joreilly@intelcomarl |
| | (Email AND Società) OR | Email Società | joreilly@intelcomintel |

## Chiavi di corrispondenza utilizzate dalle regole di corrispondenza standard

Le chiavi di corrispondenza consentono di aumentare l'efficacia delle regole di corrispondenza. Esaminare le informazioni sulle chiavi di corrispondenza per comprendere meglio il funzionamento delle regole di corrispondenza standard.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

### Che cos'è una chiave di corrispondenza?

Una *chiave di corrispondenza* è un codice che consente a una regola di corrispondenza di restituire rapidamente un elenco di possibili duplicati. Una volta attivata la regola di corrispondenza, il codice viene automaticamente applicato a tutti i record esistenti in modo tale che quando viene eseguita, la regola di corrispondenza cerchi i duplicati solo tra i record con la stessa chiave di corrispondenza. Questo processo, noto anche come indicizzazione, ottimizza le prestazioni e restituisce un insieme di candidati più pertinenti per la corrispondenza.

### Come leggere una chiave di corrispondenza



- Il campo utilizzato nella chiave di corrispondenza (1)
- Numero di token (o insiemi di stringhe di caratteri) nel valore del campo da includere nella chiave di corrispondenza (2). Se non è presente alcun numero, vengono inclusi tutti i token.

- Numero di caratteri per token da includere nella chiave di corrispondenza (3). Se non è presente alcun numero, vengono inclusi tutti i caratteri.
- Campo aggiuntivo utilizzato nella chiave di corrispondenza (4)

## Normalizzazione dei campi

Prima di applicare le chiavi di corrispondenza ai record, i valori dei campi dei record vengono normalizzati.

| Campo | Dettagli della normalizzazione | Esempi |
|---|---|---|
| Società | Espande gli acronimi. Imposta in minuscolo la prima lettera di ogni parola. Rimuove i suffissi, ad esempio `Corporation`, `Incorporated`, `Inc`, `Limited`, `Ltd`. Rimuove le stopword `e`, `il`, `di`. | IBM = international business machines<br>Intel Corp. = intel |
| Nome | Rimuove i saluti e tutte le lettere tranne la prima della prima parola. Imposta in minuscolo la prima lettera. Sostituisce il nome con un alias, se applicabile. | Dr. Jane = j<br>Mr. Bob= robert = r |
| Cognome | Rimuove caratteri speciali e suffissi. Sostituisce le consonanti consecutive identiche con una sola consonante. Imposta in minuscolo la prima lettera. Dopo la normalizzazione, viene applicato il doppio algoritmo Metaphone in modo tale che vengano considerati eventuali errori di ortografia e altre varianti. | O'Reilly, Jr. = oreily (senza doppio Metaphone)<br>O'Reilly, Jr. = oreily = arl (con doppio Metaphone) |
| Email | Rimuove i caratteri speciali, come sottolineature e punti, da entrambe le parti dell'indirizzo email. | john_doe @salesforce.com = jdoe@salesforcecom<br>john.doe@us.salesforce.com = jdoe@salesforcecom |
| Telefono | Rimuove tutti i caratteri non alfanumerici. Per i numeri di telefono degli Stati Uniti, converte i caratteri alfabetici in caratteri numerici e rimuove il codice internazionale. Rimuove le ultime quattro cifre. | 1-800-555-1234 = 800555<br>44 20 0540 0202 = 44200540 |
| Sito Web | Rimuove protocollo (http), sottodominio (www) ed eventuali percorsi di file. Quindi considera solo gli ultimi due o tre token, a seconda se esistono designazioni internazionali. | http://www.us.salesforce.com/product = salesforce.com<br>http://www.ox.ac.uk/ = ox.ac.uk |

## Chiavi di corrispondenza predefinite

Una volta normalizzati i campi, le seguenti chiavi di corrispondenza vengono applicate a tutti i record esistenti. Noto anche come indicizzazione, questo processo si verifica quando viene attivata una regola di corrispondenza.

| Chiave di corrispondenza | Oggetti di applicazione | Esempio |
|---|---|---|
| Company (2,6) City (_, 6) | Account | Account: salesforce.com = salesf<br>City: San Francisco = sanfra<br>Chiave: salesfsanfra |

| Chiave di corrispondenza | Oggetti di applicazione | Esempio |
| --- | --- | --- |
| Company (2,6) ZIP (1,3) | Account | Nome account: salesforce.com = salesf<br>ZIP: 94105-5188 = 941<br>Chiave: salesf941 |
| Email | Referente<br>Lead | Email: john_doe@us.ibm.com = johndoe@ibm.com<br>Chiave: johndoe@ibm.com |
| First_Name (1,1) Last_Name Email | Referente<br>Lead | Nome: John = j<br>Cognome: Doe = doe = t (con applicazione doppio Metaphone)<br>Email: john_doe@us.salesforce.com = johndoe@salesforce.com<br>Chiave: jt@salesforce.com |
| First_Name (1,1) Last_Name Company (2,5) | Referente<br>Lead | Nome: Marc = m<br>Cognome: Benioff = pnf (con applicazione doppio Metaphone)<br>Società: salesforce.com = sales<br>Chiave: mpnfsales |
| First_Name (1,1) Last_Name Phone | Referente<br>Lead | Nome: Marc = m<br>Cognome: Benioff = pnf (con applicazione doppio Metaphone)<br>Telefono: 1-415-555-1234 = 415555<br>Chiave: mpnf415555 |
| First_name (1,1) Last_Name Email (domain) | Referente<br>Lead | Nome: Marc = m<br>Cognome: Benioff = pnf (con applicazione doppio Metaphone)<br>Email: marc.benioff@salesforce.com = salesforce.com<br>Chiave: mpnfsalesforce.com |
| Website City (_,6) | Account | Sito Web: https://www.salesforce.com = salesforce.com<br>City: San Francisco = sanfra<br>Chiave: salesforce.comsanfra |
| Website ZIP (1,3) | Account | Sito Web: https://www.salesforce.com = salesforce.com<br>ZIP: 94105-5188 = 941<br>Chiave: salesforce.com941 |

# Domande frequenti sulla gestione dei duplicati

Risposte alle domande più comuni sulla Gestione dei duplicati di Data.com.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

IN QUESTA SEZIONE:



## Come si possono impedire i duplicati con Data.com Prospector e Pulitura Data.com?

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

### Aggiunta di record con Data.com Prospector

Dipende dalle preferenze di Data.com relative ai duplicati nell'organizzazione.

Se l'organizzazione non consente di aggiungere record duplicati a Salesforce da Data.com, Data.com impedirà l'aggiunta dei record duplicati a Salesforce e non sarà necessario eseguire la regola di duplicazione. L'utente che tenta di aggiungere i record da Data.com riceverà un registro errori in cui vengono indicati i record che non è stato possibile aggiungere perché sono duplicati.

Se l'organizzazione consente l'aggiunta dei record duplicati a Salesforce da Data.com, verranno applicate le regole di duplicazione. La regola di duplicazione determinerà se il record duplicato è consentito o bloccato. I record bloccati dalla regola di duplicazione appariranno nel registro errori.

### Aggiornamento dei record con Pulitura Data.com

Dipende dalle regole di duplicazione dell'organizzazione. Se la regola di duplicazione è impostata in modo da bloccare i duplicati in fase di modifica, non sarà possibile pulire un record se la pulitura crea un duplicato.

Per i processi di pulitura, se la regola di duplicazione è impostata in modo da bloccare o avvisare, non sarà possibile pulire un record se la pulitura crea un duplicato. Viene visualizzato un errore di entità nella tabella Cronologia processi di pulitura per ogni record che non è stato possibile pulire durante un processo.

Se la regola di duplicazione è impostata in modo da consentire i duplicati in fase di modifica, sarà possibile pulire un record anche se crea un duplicato. Inoltre, non vengono visualizzati avvisi quando si puliscono manualmente i record, nemmeno se la regola di duplicazione è impostata in modo da generare un avviso.

## Perché appare un messaggio di errore che dice che la mia regola di corrispondenza utilizza troppi operatori OR nei raggruppamenti?

Una regola di corrispondenza ha un limite di 10 campi organizzati in un'equazione. Quando viene salvata una regola di corrispondenza, l'equazione viene riscritta in un formato standardizzato che traduce le istruzioni OR in istruzioni AND. Il formato standardizzato ha un limite di 10 righe.

**Esempio:** Se la regola di corrispondenza include la seguente equazione:

(Campo 1 OR Campo 2) AND

(Campo 3 OR Campo 4) AND

(Campo 5 OR Campo 6) AND

(Campo 7 OR Campo 8)

verrà riscritta in questo modo:

(Campo 1 AND Campo 3 AND Campo 5 AND Campo 7) OR

(Campo 1 AND Campo 3 AND Campo 5 AND Campo 8) OR

(Campo 1 AND Campo 3 AND Campo 6 AND Campo 7) OR

(Campo 1 AND Campo 3 AND Campo 6 AND Campo 8) OR

(Campo 1 AND Campo 4 AND Campo 5 AND Campo 7) OR

(Campo 1 AND Campo 4 AND Campo 5 AND Campo 8) OR

(Campo 1 AND Campo 4 AND Campo 6 AND Campo 7) OR

(Campo 1 AND Campo 4 AND Campo 6 AND Campo 8) OR

(Campo 2 AND Campo 3 AND Campo 5 AND Campo 7) OR

(Campo 2 AND Campo 3 AND Campo 5 AND Campo 8) OR

(Campo 2 AND Campo 3 AND Campo 6 AND Campo 7) OR

(Campo 2 AND Campo 3 AND Campo 6 AND Campo 8) OR

(Campo 2 AND Campo 4 AND Campo 5 AND Campo 7) OR

(Campo 2 AND Campo 4 AND Campo 5 AND Campo 8) OR

(Campo 2 AND Campo 4 AND Campo 6 AND Campo 7) OR

(Campo 2 AND Campo 4 AND Campo 6 AND Campo 8)

Benché questa regola di corrispondenza rientri nel limite di campi, supera il limite di 10 righe se scritta nel formato standardizzato e quindi non può essere salvata. È necessario perfezionare la regola di corrispondenza in modo che utilizzi meno operatori OR nei raggruppamenti.

VEDERE ANCHE:

Chiavi di corrispondenza e regole di corrispondenza

# Protezione

## Panoramica sulla protezione

Salesforce dispone di una protezione integrata per i dati e le applicazioni. È anche possibile implementare un proprio schema di protezione adeguato alle esigenze dell'organizzazione. La protezione dei dati è una responsabilità comune fra l'utente e Salesforce. Le funzioni di protezione di Salesforce consentono agli utenti di svolgere le proprie attività in modo sicuro ed efficiente.

Salesforce limita l'esposizione dei dati agli utenti che li utilizzano. Implementare i controlli di protezione che si ritengono appropriati in base alla riservatezza dei propri dati. I dati sono protetti dall'accesso non autorizzato eseguito dall'esterno dell'azienda, nonché dall'utilizzo inappropriato da parte degli utenti.

Per informazioni sui vari componenti di protezione in Salesforce, vedere i seguenti argomenti:

- Affidabilità e Salesforce
- Infrastruttura di protezione
- Controllo
- Funzionamento di Crittografia piattaforma
- Protezione della sessione
- Panoramica sull'autenticazione degli utenti
- Panoramica su Single Sign-On
- Protezione a livello di rete
- Protezione CAPTCHA per l'esportazione dati
- Panoramica su Dominio personale
- Informazioni sui provider di identità e i fornitori di servizi
- Password
- Protezione dell'accesso ai dati

# Affidabilità e Salesforce

La fiducia inizia con la trasparenza. Ecco perché Salesforce visualizza informazioni in tempo reale sulle prestazioni del sistema e la sicurezza nel sito trust all'indirizzo http://trust.salesforce.com. Il sito fornisce dati aggiornati sulle prestazioni del sistema, avvisi sui tentativi attuali e recenti di phishing e malware e suggerimenti sulle procedure consigliate per la protezione dell'organizzazione.

La scheda Security nel sito trust include informazioni importanti che possono aiutare l'utente a proteggere i dati dell'azienda. In particolare, il phishing e i malware sono minacce Internet in aumento.

Il phishing è una tecnica di ingegneria sociale che tenta di acquisire informazioni critiche come nomi utente, password e dettagli delle carte di credito fingendosi un'entità affidabile nelle comunicazioni elettroniche. Gli autori di phishing spesso inducono gli utenti a immettere i propri dettagli in un sito Web falsificato che possiede un URL e un aspetto pressoché identici a quelli autentici. La comunità di Salesforce è in crescita e rappresenta pertanto un obiettivo attraente per gli utenti malintenzionati. L'utente non riceverà mai un messaggio email o una telefonata da parte di un dipendente di Salesforce con la richiesta di una password, perciò è necessario evitare di rivelare tali informazioni. Le attività sospette possono essere segnalate facendo clic sul link **Report a Suspicious Email** nella scheda **Trust** di http://trust.salesforce.com.

Il malware è un software progettato per infiltrarsi o danneggiare un sistema informatico all'insaputa del proprietario. Si tratta di un termine generale che descrive varie forme di software ostili, intrusivi o indesiderati e include i virus informatici e gli spyware.

## Cosa fa Salesforce

La protezione dei clienti è alla base del loro successo, pertanto Salesforce continuerà a implementare le migliori procedure e tecnologie disponibili in questo settore. Le azioni recenti e in corso includono:

- Monitoraggio attivo e analisi dei registri per abilitare avvisi proattivi diretti a informare i clienti interessati.
- Collaborazione con importanti fornitori ed esperti di sistemi di sicurezza in merito a specifiche minacce.
- Esecuzione di strategie rapide per eliminare o disabilitare i siti fraudolenti (spesso, entro un'ora dal rilevamento).
- Rafforzamento della formazione in materia di sicurezza e criteri di accesso più severi all'interno di Salesforce.
- Valutazione e sviluppo di nuove tecnologie, sia per i nostri clienti che per la distribuzione all'interno della nostra infrastruttura.

## Salesforce consiglia

Salesforce si impegna per stabilire i massimi standard in materia di software come servizio proponendosi come partner efficiente nella protezione dei clienti. Pertanto, oltre agli sforzi compiuti internamente, Salesforce consiglia vivamente ai clienti di implementare le modifiche descritte di seguito per rafforzare la protezione.

- Modificare la propria implementazione Salesforce per attivare le restrizioni degli intervalli IP. Ciò consente agli utenti di accedere a Salesforce solo dalla rete aziendale o VPN. Per ulteriori informazioni, vedere Impostazione delle restrizioni di accesso a pagina 515.
- Impostare delle limitazioni di sicurezza per le sessioni per rendere più difficile lo spoofing. Per ulteriori informazioni, vedere Modifica delle impostazioni di protezione della sessione a pagina 504.
- Addestrare i propri dipendenti in modo che non aprano messaggi email sospetti e prestino attenzione a eventuali tentativi di phishing.
- Utilizzare soluzioni di sicurezza di fornitori affidabili quali Symantec per distribuire filtri antispam e protezione da malware.
- Designare un referente di protezione all'interno dell'organizzazione, per facilitare la comunicazione con Salesforce. Contattare il rappresentante Salesforce con tali informazioni.
- Valutare l'utilizzo delle tecniche di autenticazione a due fattori, quali i token RSA, per restringere l'accesso alla propria rete. Per ulteriori informazioni, vedere Autenticazione a due fattori in Salesforce a pagina 517

Salesforce dispone di un team di intervento in caso di minacce alla sicurezza per gestire le problematiche di protezione. Per segnalare una minaccia alla protezione di Salesforce, contattare security@salesforce.com. Descrivere dettagliatamente il problema per consentire al team di intervenire rapidamente.

# Infrastruttura di protezione

Una delle funzionalità essenziali di una piattaforma multi-tenant è l'utilizzo di un gruppo unico di risorse di calcolo per soddisfare le esigenze di molti utenti diversi. Salesforce protegge i dati dell'organizzazione da tutte le altre organizzazioni del cliente utilizzando un ID dell'organizzazione univoco, associato a ogni sessione dell'utente. Dopo aver effettuato l'accesso alla propria organizzazione, le successive richieste dell'utente vengono associate all'organizzazione utilizzando tale ID.

Salesforce utilizza alcune delle tecnologie di protezione Internet più avanzate disponibili al giorno d'oggi. Quando si accede all'applicazione utilizzando un browser supportato da Salesforce, la tecnologia TLS (Transport Layer Security) protegge le informazioni dell'utente utilizzando sia l'autenticazione del server che la Crittografia classica, garantendo che i dati siano protetti e disponibili solo agli utenti registrati della propria organizzazione.

Inoltre, Salesforce è ospitato in un ambiente server protetto che utilizza un firewall e altre tecnologie avanzate per prevenire interferenze o accessi dall'esterno.

# Controllo

Le funzioni di controllo non sono sufficienti, da sole, a proteggere l'organizzazione, ma forniscono informazioni sull'utilizzo del sistema, che possono essere fondamentali per diagnosticare problematiche di sicurezza potenziali o reali. È importante che un membro dell'organizzazione svolga controlli regolari per rilevare potenziali abusi. Le altre funzioni di protezione fornite da Salesforce sono preventive. Per verificare l'effettiva sicurezza del sistema, eseguire controlli per monitorare le modifiche impreviste o le tendenze di utilizzo.

Le funzioni di controllo comprendono:

**Campi di modifica dei record**

Tutti gli oggetti includono campi per l'archiviazione del nome dell'utente che ha creato il record e dell'utente che lo ha modificato per ultimo. In questo modo è possibile fornire alcune informazioni di controllo di base.

**Cronologia accessi**

È possibile visualizzare un elenco dei tentativi di accesso all'organizzazione, riusciti e non riusciti, degli ultimi sei mesi. Vedere Monitoraggio della cronologia accessi a pagina 668.

**Tracciamento della cronologia dei campi**

È anche possibile attivare il controllo per i singoli campi, per tracciare automaticamente le modifiche nei valori dei campi selezionati. Benché il controllo sia disponibile per tutti gli oggetti personalizzati, solo alcuni oggetti standard consentono il controllo a livello di campo. Vedere Tracciamento della cronologia dei campi a pagina 673.

**Itinerario di controllo impostazioni**

Gli amministratori possono anche visualizzare un Itinerario di controllo impostazioni, che registra quando vengono apportate modifiche alla configurazione dell'organizzazione. Vedere Monitoraggio delle modifiche di impostazione a pagina 670.

# Crittografia piattaforma

## Protezione dei dati con Crittografia piattaforma

Per utilizzare Crittografia piattaforma nella propria organizzazione, iniziare con la creazione di un segreto tenant. In seguito si indicheranno i campi e i file da crittografare e si designeranno gli utenti incaricati della generazione, rotazione e archiviazione delle chiavi dell'organizzazione.

EDIZIONI

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**
Disponibile gratuitamente nella versione **Developer Edition** per le organizzazioni create a partire dal rilascio Summer '15.

AUTORIZZAZIONI UTENTE

Per gestire i segreti tenant:
- "Gestisci chiavi di crittografia"

IN QUESTA SEZIONE:

1. Gestione dei segreti tenant e delle chiavi

   Con Crittografia piattaforma ogni organizzazione gestisce il suo segreto tenant, che utilizza per derivare le chiavi che proteggono i dati. Dopo avere creato un segreto tenant esclusivo per la propria organizzazione è possibile farlo ruotare, archiviarlo e condividerne la responsabilità con altri utenti.

2. Crittografia dei campi

   Selezionare i campi che si desidera crittografare. Quando un campo è crittografato, il suo valore è riprodotto con degli asterischi agli utenti che non sono autorizzati a visualizzarlo.

3. Crittografia di file e allegati

   Per una maggiore protezione dei dati, crittografare file e allegati utilizzando Crittografia piattaforma. Quando Crittografia piattaforma è abilitata, il corpo dei file e degli allegati viene crittografato in sede di caricamento.

4. Disattivazione di Crittografia piattaforma

   In alcuni casi può essere necessario disabilitare Crittografia piattaforma per i campi, per i file o per entrambi. Quando si disattiva Crittografia piattaforma, i dati crittografati non vengono decrittografati globalmente e le eventuali funzionalità interessate dalla crittografia non vengono ripristinate. Per assistenza, rivolgersi a Salesforce.

## Gestione dei segreti tenant e delle chiavi

Con Crittografia piattaforma ogni organizzazione gestisce il suo segreto tenant, che utilizza per derivare le chiavi che proteggono i dati. Dopo avere creato un segreto tenant esclusivo per la propria organizzazione è possibile farlo ruotare, archiviarlo e condividerne la responsabilità con altri utenti.

Gli utenti autorizzati generano i segreti tenant su richiesta dalla pagina di Crittografia piattaforma. Gli sviluppatori autorizzati li possono generare inserendo nel codice una chiamata all'oggetto TenantSecret nell'API Salesforce.

AUTORIZZAZIONI UTENTE

Per gestire i segreti tenant:
- "Gestisci chiavi di crittografia"

Le chiavi di crittografia dei dati non vengono mai condivise tra un'organizzazione e l'altra o salvate su disco. Vengono invece derivate su richiesta a partire da un segreto master e da un segreto tenant specifico dell'organizzazione e quindi inserite nella cache di un server di applicazioni.

IN QUESTA SEZIONE:



VEDERE ANCHE:

Autorizzazioni utente per Crittografia piattaforma

https://developer.salesforce.com/docs/atlas.en-us.api.meta/api/sforce_api_objects_tenantsecret.htm

Torna all'argomento principale

Autorizzazioni utente per Crittografia piattaforma

https://developer.salesforce.com/docs/atlas.en-us.api.meta/api/sforce_api_objects_tenantsecret.htm

Torna all'argomento principale

## Creazione di un segreto tenant

Creare un segreto tenant esclusivo per l'organizzazione e quindi autorizzare persone specifiche a usarlo per generare nuove chiavi di crittografia dei dati.

AUTORIZZAZIONI UTENTE

Per gestire i segreti tenant:
- "Gestisci chiavi di crittografia"

1. Creare il segreto tenant.
   a. Da Imposta, immettere *Crittografia piattaforma* nella casella Ricerca veloce, quindi selezionare **Crittografia piattaforma**.
   b. Fare clic su **Crea segreto tenant**.
2. Assegnare l'autorizzazione "Gestisci chiavi di crittografia" a persone fidate per la gestione dei segreti tenant dell'organizzazione.

   Questa autorizzazione si può aggiungere a un profilo o a un insieme di autorizzazioni: da Imposta, immettere *Profili* o *Insiemi di autorizzazioni* nella casella Ricerca veloce.

   Nota: Per gli amministratori, l'autorizzazione "Gestisci chiavi di crittografia" è abilitata per impostazione predefinita.

Nota: queste informazioni sono valide per Crittografia piattaforma e non per la crittografia classica.

VEDERE ANCHE:

Insiemi di autorizzazioni
Profili
Insiemi di autorizzazioni
Profili

## Rotazione della chiave di Crittografia piattaforma

EDIZIONI

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

Disponibile gratuitamente nella versione **Developer Edition** per le organizzazioni create a partire dal rilascio Summer '15.

AUTORIZZAZIONI UTENTE

Per gestire i segreti tenant:

- "Gestisci chiavi di crittografia"

La rotazione della chiave è il processo di generazione di un nuovo segreto tenant e di archiviazione di quello attivo in precedenza. Controllando il ciclo di vita dei segreti tenant dell'organizzazione si controlla il ciclo di vita delle chiavi di crittografia dei dati derivate.

La rotazione della chiave è determinata dalle policy di sicurezza dell'organizzazione. In un'organizzazione di produzione la rotazione del segreto tenant può avvenire ogni 24 ore, e ogni quattro ore in un ambiente Sandbox. La rotazione dei segreti master utilizzati nella funzione di derivazione delle chiavi avviene a ogni rilascio principale di Salesforce. Questo non influisce sulle chiavi cliente né sui dati crittografati fino a quando non viene eseguita la rotazione del segreto tenant.

1. Per controllare lo stato delle chiavi dell'organizzazione, da Imposta immettere *Crittografia piattaforma* nella casella `Ricerca veloce`, quindi selezionare **Crittografia piattaforma**. Le chiavi possono essere attive, archiviate o distrutte.

   **ATTIVO**
   
   La chiave si può utilizzare per crittografare e decrittografare dati nuovi o esistenti.

   **ARCHIVIATO**
   
   Non è possibile crittografare nuovi dati. Si può utilizzare per decrittografare i dati precedentemente crittografati con la stessa chiave quando era attiva.

   **DISTRUTTO**
   
   La chiave non può crittografare o decrittografare dati. I dati crittografati quando questa chiave era attiva non possono più essere decrittografati.

2. Da Imposta, immettere *Crittografia piattaforma* nella casella `Ricerca veloce`, quindi selezionare **Crittografia piattaforma**.
3. Fare clic su **Genera nuovo segreto tenant**.
4. se si desidera crittografare nuovamente i valori dei campi esistenti con un segreto tenant appena generato, modificare e salvare i campi crittografati mediante Data Loader o un altro strumento.

   Provocare l'aggiornamento dei dati esportando gli oggetti tramite l'API o eseguendo un rapporto che contenga l'ID del record. In questo modo si attiva il servizio di crittografia che crittografa nuovamente i dati esistenti usando la chiave più recente.

Nota: le informazioni che seguono sono valide per Crittografia piattaforma e non per la crittografia classica.

## Esportazione e importazione di un segreto tenant

Il segreto tenant è esclusivo dell'organizzazione e dei dati specifici per cui è valido. Salesforce consiglia di esportare il segreto tenant per garantire l'accesso continuativo ai dati nei casi in cui sia necessario accedere nuovamente ai dati correlati.

1. Da Imposta, immettere *`Crittografia piattaforma`* nella casella `Ricerca veloce`, quindi selezionare **Crittografia piattaforma**.
2. Nella tabella con l'elenco delle chiavi, trovare il segreto tenant desiderato e fare clic su **Esporta**.
3. Confermare la scelta nella finestra di avviso e salvare il file esportato.

   Il nome del file è `tenant-secret-org-<ID organizzazione>-ver-<numero versione segreto tenant>.txt`. Ad esempio, `tenant-secret-org-00DD00000007eTR-ver-1.txt`.
4. Prendere nota della versione specifica esportata e assegnare al file esportato un nome significativo. Archiviare il file in luogo sicuro qualora sia necessario reimportarlo nell'organizzazione.

   Nota: il segreto tenant esportato viene crittografato.
5. Per reimportare il segreto tenant, fare clic su **Importa** > **Scegli file** e selezionare il file. Controllare che la versione del segreto tenant da importare sia quella corretta.

EDIZIONI

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

Disponibile gratuitamente nella versione **Developer Edition** per le organizzazioni create a partire dal rilascio Summer '15.

AUTORIZZAZIONI UTENTE

Per gestire i segreti tenant:
- "Gestisci chiavi di crittografia"

Nota: le informazioni che seguono sono valide per Crittografia piattaforma e non per la crittografia classica.

## Distruzione di un segreto tenant

Distruggere i segreti tenant solo in casi estremi in cui non è più necessario l'accesso ai dati correlati. il segreto tenant è esclusivo dell'organizzazione e dei dati specifici per cui è valido. Dopo che un segreto tenant è stato distrutto, i dati correlati non saranno più accessibili a meno che la chiave non sia stata precedentemente esportata e reimportata in Salesforce.

Nota: se si crea un'organizzazione Sandbox dall'organizzazione di produzione e poi si distrugge il segreto tenant nell'organizzazione Sandbox, il segreto tenant viene mantenuto senza alcuna modifica nell'organizzazione di produzione.

1. Da Imposta, immettere *`Crittografia piattaforma`* nella casella `Ricerca veloce`, quindi selezionare **Crittografia piattaforma**.
2. Nella tabella contenente l'elenco dei segreti tenant, passare alla riga del segreto tenant che si desidera distruggere e fare clic su **Distruggi**.
3. Viene visualizzata una finestra di avviso. Se si tratta del segreto tenant che si desidera distruggere:
   a. Digitare il testo indicato.
   b. Selezionare la casella di controllo per confermare la distruzione del segreto tenant.
   c. Fare clic su **Distruggi**.

EDIZIONI

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

Disponibile gratuitamente nella versione **Developer Edition** per le organizzazioni create a partire dal rilascio Summer '15.

AUTORIZZAZIONI UTENTE

Per gestire i segreti tenant:
- "Gestisci chiavi di crittografia"

Nota: le informazioni che seguono sono valide per Crittografia piattaforma e non per la crittografia classica.

## Crittografia dei campi

Selezionare i campi che si desidera crittografare. Quando un campo è crittografato, il suo valore è riprodotto con degli asterischi agli utenti che non sono autorizzati a visualizzarlo.

L'abilitazione di un campo standard per la crittografia può richiedere un tempo più o meno lungo a seconda delle dimensioni dell'organizzazione.

1. Controllare che l'organizzazione disponga di una chiave di crittografia attiva. In caso di dubbi, rivolgersi all'amministratore.
2. Da Imposta, immettere *`Crittografia piattaforma`* nella casella `Ricerca veloce`, quindi selezionare **Crittografia piattaforma**.
3. Selezionare **Abilita campi standard crittografati**.
4. Selezionare **Modifica**.
5. Selezionare i campi da crittografare e salvare le impostazioni.

Viene avviato il servizio di convalida automatica di Crittografia piattaforma. Se qualche impostazione dell'organizzazione blocca la crittografia, si riceverà un messaggio email contenente le istruzioni per eliminare l'inconveniente.

I valori dei campi vengono crittografati automaticamente solo nei record creati o aggiornati dopo l'abilitazione della crittografia. Salesforce consiglia di aggiornare i record esistenti per assicurarsi che i valori dei campi vengano crittografati. Ad esempio, se si crittografa il campo `Descrizione` nell'oggetto Caso, utilizzare Data Loader per aggiornare tutti i record caso. Per assistenza, rivolgersi a Salesforce.

Nota: le informazioni che seguono sono valide per Crittografia piattaforma e non per la crittografia classica.

EDIZIONI

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

Disponibile gratuitamente nella versione **Developer Edition** per le organizzazioni create a partire dal rilascio Summer '15.

AUTORIZZAZIONI UTENTE

Per visualizzare l'impostazione:

- "Visualizza impostazione e configurazione"

Per abilitare i campi crittografati:

- "Personalizza applicazione"

VEDERE ANCHE:

Quali campi si possono crittografare?
Su alcuni campi, la crittografia ha conseguenze inattese
Data Loader
Convalida automatica per Crittografia piattaforma
Torna all'argomento principale
Quali campi si possono crittografare?
Su alcuni campi, la crittografia ha conseguenze inattese
Data Loader
Convalida automatica per Crittografia piattaforma
Torna all'argomento principale

## Crittografia di file e allegati

Per una maggiore protezione dei dati, crittografare file e allegati utilizzando Crittografia piattaforma. Quando Crittografia piattaforma è abilitata, il corpo dei file e degli allegati viene crittografato in sede di caricamento.

EDIZIONI

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

Disponibile gratuitamente nella versione **Developer Edition** per le organizzazioni create a partire dal rilascio Summer '15.

AUTORIZZAZIONI UTENTE

Per visualizzare l'impostazione:
- "Visualizza impostazione e configurazione"

Per abilitare i campi crittografati:
- "Personalizza applicazione"

Nota: prima di iniziare, assicurarsi che l'organizzazione disponga di una chiave di crittografia attiva; in caso di dubbio, rivolgersi all'amministratore.

È possibile crittografare i seguenti tipi di file:

- File allegati ai feed
- File allegati ai record
- File nelle schede Contenuto, Librerie e File (file Chatter, incluse le anteprime dei file e i file di Salesforce CRM Content)
- File gestiti con Salesforce Files Sync
- Note (Beta)

Alcuni tipi di file e allegati non si possono crittografare:

- Gruppi Chatter e foto di profili
- Documenti
- Allegati email

1. Da Imposta, immettere `Crittografia piattaforma` nella casella `Ricerca veloce`, quindi selezionare **Crittografia piattaforma**.
2. Selezionare **Abilita file e allegati crittografati**.
3. Fare clic su **Imposta preferenze**.

Importante: gli utenti autorizzati ad accedere al file possono utilizzarlo normalmente indipendentemente dalle loro autorizzazioni specifiche per la crittografia. Gli utenti che si sono autenticati nell'organizzazione e che hanno accesso in lettura possono visualizzare il contenuto del corpo dei file ed eseguirvi ricerche.

Gli utenti possono continuare a caricare file e allegati con i normali limiti di dimensioni dei file. L'eventuale aumento delle dimensioni dei file causato dalla crittografia non ha effetto su tali limiti.

L'attivazione della crittografia di file e allegati interessa i nuovi file e allegati. I file e gli allegati già presenti in Salesforce non vengono invece crittografati. Per crittografare i file esistenti, rivolgersi a Salesforce.

Per verificare se un file o un allegato è crittografato, cercare l'indicatore di crittografia nella pagina dei dettagli del file o dell'allegato o eseguire una query sul campo `isEncrypted` nell'oggetto ContentVersion (per i file) o nell'oggetto Allegati (per gli allegati).

**Aspetto della pagina dei dettagli di un file crittografato**

**Nota:** le informazioni che seguono sono valide per Crittografia piattaforma e non per la crittografia classica.

VEDERE ANCHE:

Convalida automatica per Crittografia piattaforma
Torna all'argomento principale
Convalida automatica per Crittografia piattaforma
Torna all'argomento principale

## Disattivazione di Crittografia piattaforma

In alcuni casi può essere necessario disabilitare Crittografia piattaforma per i campi, per i file o per entrambi. Quando si disattiva Crittografia piattaforma, i dati crittografati non vengono decrittografati globalmente e le eventuali funzionalità interessate dalla crittografia non vengono ripristinate. Per assistenza, rivolgersi a Salesforce.

Ad esempio, può essere necessario disabilitare la crittografia su un campo in modo che gli utenti sprovvisti di autorizzazione "Visualizza dati crittografati" possano visualizzare i dati senza mascheramento.

1. Da Imposta, immettere *Crittografia piattaforma* nella casella Ricerca veloce, quindi selezionare **Crittografia piattaforma**.
2. Deselezionare i campi da rendere visibili agli utenti senza autorizzazione "Visualizza dati crittografati".
3. Per disabilitare completamente la crittografia dei campi, deselezionare **Abilita campi standard crittografati**.
4. Per disabilitare la crittografia per i file, selezionare **Disabilita file e allegati crittografati**.

Le limitazioni e i comportamenti speciali validi per i campi crittografati rimangono validi dopo la disabilitazione della crittografia. I valori possono rimanere crittografati a riposo e mascherati in alcuni punti. Tutti i file e gli allegati precedentemente crittografati rimangono crittografati a riposo.

I campi crittografati rimangono accessibili dopo la disabilitazione della crittografia a patto che la chiave utilizzata per crittografarli non venga distrutta.

VEDERE ANCHE:

Torna all'argomento principale

Torna all'argomento principale

## Funzionamento di Crittografia piattaforma

EDIZIONI

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

Disponibile gratuitamente nella versione **Developer Edition** per le organizzazioni create a partire dal rilascio Summer '15.

Crittografia piattaforma garantisce ai dati un nuovo livello di protezione, conservando le funzionalità cruciali della piattaforma. I dati selezionati vengono crittografati a riposo mediante un sistema avanzato di derivazione delle chiavi. Così è possibile proteggere i dati a un livello di dettaglio mai raggiunto prima. Crittografia piattaforma consente alla società di conformarsi in tutta tranquillità ai criteri per la tutela della privacy, ai requisiti di legge e agli obblighi contrattuali per la manipolazione di dati privati.

Crittografia piattaforma si aggiunge alle opzioni di crittografia dei dati di base disponibili in Salesforce. Permette di crittografare i dati memorizzati in molti campi standard e personalizzati e in file e allegati. I dati vengono crittografati a riposo, non solo quando vengono trasmessi in rete, e quindi sono protetti anche dopo che altre linee di difesa sono state compromesse.

La crittografia di file, campi e allegati non ha alcun effetto sui limiti di memoria dell'organizzazione.

Nota: le informazioni che seguono sono valide per Crittografia piattaforma e non per la crittografia classica.

IN QUESTA SEZIONE:

Procedure consigliate per Crittografia piattaforma

Dedicare un po' di tempo all'identificazione delle minacce più probabili per la propria organizzazione. In questo modo sarà più facile distinguere i dati che richiedono la crittografia da quelli che non la richiedono e usare la crittografia solo dove è necessario. Accertarsi di avere fatto un backup del segreto tenant e delle chiavi e scegliere con attenzione il responsabile della gestione dei segreti e delle chiavi.

Quali campi si possono crittografare?

Si possono crittografare alcuni campi degli oggetti Account, Referente, Caso e Commento caso. Quando è abilitato Crittografia piattaforma, gli utenti con l'autorizzazione "Visualizza dati crittografati" vedono il contenuto dei campi crittografati, mentre quelli sprovvisti dell'autorizzazione vedono solo valori mascherati (i valori vengono cioè sostituiti da un numero fisso di asterischi).

Terminologia di Crittografia piattaforma

La crittografia ha un suo vocabolario specializzato. Per utilizzare al meglio le funzioni di Crittografia piattaforma può essere utile acquisire dimestichezza con alcuni termini chiave come Hardware Security Module, rotazione della chiave e segreto master.

Il processo di Crittografia piattaforma

Quando gli utenti inviano dei dati, il server di applicazioni cerca la chiave di crittografia dei dati specifica di quell'organizzazione all'interno della sua cache. Se la chiave non è presente, il server di applicazioni recupera il segreto tenant crittografato dal database, si autentica sul server di derivazione delle chiavi su un canale protetto e chiede al server di derivare la chiave. In seguito, il servizio di crittografia crittografa i dati sul server di applicazioni.

## Procedure consigliate per Crittografia piattaforma

EDIZIONI

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

Disponibile gratuitamente nella versione **Developer Edition** per le organizzazioni create a partire dal rilascio Summer '15.

Dedicare un po' di tempo all'identificazione delle minacce più probabili per la propria organizzazione. In questo modo sarà più facile distinguere i dati che richiedono la crittografia da quelli che non la richiedono e usare la crittografia solo dove è necessario. Accertarsi di avere fatto un backup del segreto tenant e delle chiavi e scegliere con attenzione il responsabile della gestione dei segreti e delle chiavi.

IN QUESTA SEZIONE:

Procedure consigliate: distribuzione di Crittografia piattaforma agli utenti

Testare accuratamente le app prima di distribuirle. Verificare che gli utenti abbiano capito l'importanza della crittografia e i suoi potenziali effetti sul lavoro quotidiano, e valutare con attenzione quando concedere l'accesso.

VEDERE ANCHE:

Torna all'argomento principale

Torna all'argomento principale

## Procedure consigliate: operazioni preliminari per Crittografia piattaforma

Prima di iniziare a utilizzare Crittografia piattaforma, pianificare la strategia di crittografia definendo un modello di minaccia e classificando dati e utenti di conseguenza. Preparare un procedimento di backup per chiavi e dati e assicurarsi di avere compreso l'impatto della crittografia sulle normali operazioni dell'organizzazione.

1. Definire un modello di minaccia per l'organizzazione.

   Fare riferimento a un esercizio sulla creazione di un modello di minaccia formale per identificare le minacce che con maggiore probabilità possono influire sull'organizzazione. Utilizzare i risultati ottenuti per creare uno schema di classificazione dei dati, che può essere utile per scegliere i dati da crittografare.

2. Crittografare i dati solo se necessario.
   - Non tutti i dati sono sensibili. Concentrarsi su quelli che richiedono la crittografia per poter soddisfare i requisiti normativi, di sicurezza, conformità e privacy. La crittografia non necessaria ha un impatto negativo sulla funzionalità e sulle prestazioni.
   - Valutare in anticipo lo schema di classificazione dei dati in uso e collaborare con le persone coinvolte nei reparti addetti a sicurezza, conformità e IT aziendale per definire i requisiti. Allineare le funzionalità cruciali per l'azienda con le misure in termini di sicurezza e rischi e mettere periodicamente alla prova i presupposti.

3. Creare in anticipo una strategia per il backup e l'archiviazione di chiavi e dati.

   Se i segreti tenant vengono distrutti, reimportarli per accedere ai dati. Siete gli unici responsabili del backup e della conservazione dei dati e dei segreti tenant in luogo sicuro. Salesforce non può fornire assistenza in caso di eliminazione, distruzione o perdita dei segreti tenant.

4. Ricordare che la crittografia viene applicata per tutti gli utenti, indipendentemente dalle loro autorizzazioni.
   - Per stabilire chi può leggere i valori dei campi crittografati come testo normale, utilizzare l'autorizzazione "Visualizza dati crittografati". Tuttavia, i dati memorizzati in questi campi sono crittografati a riposo, indipendentemente dalle autorizzazioni degli utenti.
   - Vengono imposti alcuni limiti funzionali agli utenti che interagiscono con i dati crittografati. Valutare se la crittografia può essere applicata a una porzione degli utenti aziendali e in che modo l'applicazione può influire sugli altri utenti che interagiscono con i dati.

5. Leggere le considerazioni su Crittografia piattaforma e comprenderne le implicazioni nella propria organizzazione.
   - Valutare l'impatto delle considerazioni sulla soluzione aziendale e l'implementazione.
   - Testare Crittografia piattaforma in un ambiente Sandbox prima di distribuirla a un ambiente di produzione.
   - Prima di abilitare la crittografia, risolvere eventuali violazioni identificate. Ad esempio, fare riferimento ai campi crittografati in una clausola SOQL WHERE attiva una violazione. Analogamente, se si fa riferimento ai campi crittografati in una clausola SOQL ORDER BY, si verifica una violazione. In entrambi i casi, correggere la violazione rimuovendo i riferimenti ai campi crittografati.

6. Analizzare e testare le applicazioni AppExchange prima della distribuzione.

- Se si utilizza un'app di AppExchange, verificare in che modo interagisce con i dati crittografati nell'organizzazione e valutare se vi sono conseguenze sulla funzionalità.
- Se un'app interagisce con dati crittografati memorizzati all'esterno di Salesforce, verificare come e dove avviene l'elaborazione dei dati e in che modo sono protette le informazioni.
- Se si sospetta che Crittografia piattaforma possa influire sulla funzionalità di un'app, richiedere l'assistenza del fornitore per effettuare la valutazione. Verificare inoltre come gestire eventuali soluzioni personalizzate che devono essere compatibili con Crittografia piattaforma.
- Le app AppExchange create esclusivamente con Force.com ereditano le funzioni e i limiti di Crittografia piattaforma.

Nota: queste informazioni sono valide per Crittografia piattaforma e non per la crittografia classica.

## Procedure consigliate: impostazione di Crittografia piattaforma

EDIZIONI

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**
Disponibile gratuitamente nella versione **Developer Edition** per le organizzazioni create a partire dal rilascio Summer '15.

Quando si implementa Crittografia piattaforma, evitare di crittografare i dati che non lo richiedono. Assegnare l'autorizzazione all'uso delle funzioni di crittografia solo agli utenti che ne hanno veramente bisogno.

1. Crittografia piattaforma non è uno strumento di autorizzazione o di autenticazione degli utenti. Per controllare la visualizzazione dei dati da parte degli utenti, utilizzare le impostazioni di protezione a livello di campo, le impostazioni dei layout di pagina e le regole di convalida, ma non Crittografia piattaforma. Verificare che un utente a cui sia stata inavvertitamente concessa l'autorizzazione Visualizza dati crittografati possa comunque visualizzare solo i dati appropriati.

   Per impostazione predefinita, qualsiasi utente può modificare i campi crittografati, anche gli utenti senza autorizzazione "Visualizza dati crittografati".

2. Concedere l'autorizzazione "Gestisci chiavi di crittografia" solo agli utenti autorizzati.

   Gli utenti con autorizzazione "Gestisci chiavi di crittografia" possono generare, esportare, importare e distruggere chiavi specifiche dell'organizzazione. Monitorare regolarmente le principali attività di gestione di questi utenti con l'itinerario di controllo delle impostazioni.

3. Concedere l'autorizzazione "Visualizza dati crittografati" solo agli utenti autorizzati.

   Concedere l'autorizzazione "Visualizza dati crittografati" agli utenti che devono visualizzare i campi crittografati come testo normale, inclusi gli utenti integrazione che devono leggere i dati sensibili in formato di testo normale. i file crittografati sono visibili a tutti gli utenti che hanno accesso ai file, indipendentemente dall'autorizzazione "Visualizza dati crittografati".

4. Crittografare globalmente i dati esistenti.

   I dati dei campi e dei file già esistenti non vengono automaticamente crittografati quando si attiva Crittografia piattaforma. Per crittografare i dati dei campi esistenti, aggiornare i record associati ai dati dei campi. Questa azione attiva la crittografia per quei record, in modo tale che i dati già esistenti vengono crittografati a riposo. Per crittografare i file esistenti, rivolgersi a Salesforce.

5. Evitare la crittografia dei dati di Valuta, Numero, Data e Data/ora.

   Spesso è possibile tenere al sicuro i dati personali, sensibili o "regolati" senza crittografare i campi `Valuta`, `Numero`, `Data` e `Data/ora` associati. La crittografia di questi campi può avere notevoli conseguenze per la funzionalità di tutta la piattaforma, ad esempio interruzioni nei rapporti di riepilogo di roll-up, negli intervalli di tempo dei rapporti e nei calcoli.

Nota: queste informazioni sono valide per Crittografia piattaforma e non per la crittografia classica.

## Procedure consigliate: distribuzione di Crittografia piattaforma agli utenti

EDIZIONI

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

Disponibile gratuitamente nella versione **Developer Edition** per le organizzazioni create a partire dal rilascio Summer '15.

Testare accuratamente le app prima di distribuirle. Verificare che gli utenti abbiano capito l'importanza della crittografia e i suoi potenziali effetti sul lavoro quotidiano, e valutare con attenzione quando concedere l'accesso.

1. Comunicare agli utenti gli effetti della crittografia.

   Prima di abilitare Crittografia piattaforma in un ambiente di produzione, informare gli utenti dell'impatto previsto sulla soluzione aziendale. Ad esempio, condividere le informazioni riportate nelle considerazioni su Crittografia piattaforma quando sono rilevanti per i processi aziendali.

2. Usare discrezione quando si concede l'accesso.

   Se un utente con autorizzazione "Visualizza dati crittografati" concede l'accesso a un altro utente, l'altro utente sarà in grado di visualizzare i campi crittografati come testo normale.

3. Crittografare i dati utilizzando la chiave più recente.

   Quando si genera un nuovo segreto tenant, tutti i nuovi dati vengono crittografati utilizzando questa chiave. Tuttavia, i dati sensibili già esistenti rimangono crittografati con la chiave precedente. In questa situazione, Salesforce consiglia vivamente di crittografare di nuovo i campi utilizzando la chiave più recente. Per assistenza, rivolgersi a Salesforce.

Nota: queste informazioni sono valide per Crittografia piattaforma e non per la crittografia classica.

## Quali campi si possono crittografare?

Si possono crittografare alcuni campi degli oggetti Account, Referente, Caso e Commento caso. Quando è abilitato Crittografia piattaforma, gli utenti con l'autorizzazione "Visualizza dati crittografati" vedono il contenuto dei campi crittografati, mentre quelli sprovvisti dell'autorizzazione vedono solo valori mascherati (i valori vengono cioè sostituiti da un numero fisso di asterischi).

In ogni caso, i campi crittografati funzionano normalmente in tutta l'interfaccia, i processi aziendali e le API di Salesforce (con alcune eccezioni: ad esempio, i campi crittografati non si possono ordinare).

Quando si attiva la crittografia, i valori presenti nei campi non vengono crittografati immediatamente, ma solo dopo essere stati modificati. Per assistenza sulla crittografia dei dati esistenti, rivolgersi a Salesforce.

### Campi standard crittografati

È possibile crittografare il contenuto dei seguenti tipi di campi standard.

- Nell'oggetto Account:
  - `Nome account`
- Nell'oggetto Referente:
  - `Email`
  - `Fax`
  - `Telefono abitazione`
  - `Indirizzo postale` (vengono crittografati solo `Via indirizzo postale` e `Città indirizzo postale`)
  - `Cellulare`
  - `Nome` (vengono crittografati solo `Nome`, `Secondo nome` e `Cognome`)
  - `Altro telefono`
  - `Telefono`

- Nell'oggetto Caso:
  - `Oggetto`
  - `Descrizione`
- Nell'oggetto Commenti caso:
  - `Corpo`

### Campi personalizzati crittografati

È possibile crittografare il contenuto dei seguenti tipi di campi personalizzati:

- Email
- Telefono
- Testo
- Area di testo
- Area di testo (lungo)
- URL

**Importante:** dopo avere crittografato un campo personalizzato non sarà possibile modificarne il tipo. Per i campi personalizzati telefono ed email non sarà possibile nemmeno modificare il formato.

Non è possibile utilizzare campi personalizzati attualmente o precedentemente crittografati in campi formula personalizzati o in regole di condivisione basate sui criteri.

Non è possibile utilizzare il Generatore di schemi per creare un campo personalizzato crittografato.

Alcuni campi personalizzati non si possono crittografare:

- Campi con l'attributo `Univoco` o `ID esterno` o che includono tali attributi in campi personalizzati crittografati in precedenza.
- Campi utilizzati in campi formula personalizzati.
- Campi di oggetti di dati esterni.

**Nota:** queste informazioni sono valide per Crittografia piattaforma e non per la crittografia classica.

VEDERE ANCHE:

Crittografia dei campi

Torna all'argomento principale

Crittografia dei campi

Torna all'argomento principale

## Terminologia di Crittografia piattaforma

La crittografia ha un suo vocabolario specializzato. Per utilizzare al meglio le funzioni di Crittografia piattaforma può essere utile acquisire dimestichezza con alcuni termini chiave come Hardware Security Module, rotazione della chiave e segreto master.

**Crittografia dei dati**

Processo di applicazione di una funzione crittografica ai dati che genera testo cifrato. Il processo di Crittografia piattaforma utilizza la crittografia a chiave simmetrica e un algoritmo AES (Advanced Encryption Standard) a 256 bit con modalità CBC, padding PKCS5 e un vettore di inizializzazione (IV) randomizzato a 128 bit per crittografare i dati a livello di campo e i file archiviati nella piattaforma Salesforce. La crittografia e la decrittografia dei dati avvengono entrambe sui server di applicazioni.

**Chiavi di crittografia dei dati**

Crittografia piattaforma utilizza delle chiavi di crittografia dei dati per crittografare e decrittografare i dati. Le chiavi di crittografia dei dati vengono derivate in un server di derivazione delle chiavi utilizzando materiale per la generazione di chiavi suddiviso fra un segreto master specifico del rilascio e un segreto tenant specifico dell'organizzazione memorizzato in forma crittografata nel database come parte dell'organizzazione. Le chiavi derivate a 256 bit rimangono in memoria fino a quando non vengono eliminate dalla cache.

**Dati crittografati a riposo**

Dati che vengono crittografati quando sono memorizzati su disco. Salesforce supporta la crittografia dei campi memorizzati nel database, dei documenti archiviati in File, Librerie di contenuti e Allegati e dei dati archiviati.

**Gestione delle chiavi di crittografia**

Include tutte le operazioni di gestione delle chiavi, ad esempio la creazione delle chiavi, i processi e l'archiviazione. La gestione dei segreti tenant è compito degli amministratori o degli utenti dotati di autorizzazione "Gestisci chiavi di crittografia", che si abilita da Imposta immettendo *Crittografia piattaforma* nella casella Ricerca veloce e selezionando quindi **Crittografia piattaforma**.

**HSM (Hardware Security Module, modulo di protezione hardware)**

Utilizzato per l'elaborazione della crittografia e la gestione delle chiavi per l'autenticazione. Crittografia piattaforma utilizza gli HSM per generare e memorizzare il materiale segreto ed eseguire la funzione di derivazione delle chiavi di crittografia dei dati utilizzate dal servizio di crittografia per crittografare e decrittografare i dati.

**VI (vettore di inizializzazione)**

Sequenza casuale utilizzata con una chiave per crittografare i dati.

**Funzione di derivazione delle chiavi (KDF, Key Derivation Function)**

Utilizza un generatore di numeri pseudocasuali e input come una password per derivare le chiavi. Crittografia piattaforma utilizza PBKDF2 (Password-based Key Derivation Function 2) con HMAC-SHA-256.

**Rotazione della chiave (segreto tenant)**

Processo di generazione di un nuovo segreto tenant e di archiviazione di quello precedentemente attivo. I segreti tenant attivi vengono utilizzati sia per la crittografia, sia per la decrittografia. I segreti tenant archiviati vengono utilizzati solo per la decrittografia fino a quando tutti i dati non siano stati nuovamente crittografati con il nuovo segreto tenant attivo.

**HSM principale**

L'HSM principale è costituito da un dispositivo USB utilizzato per generare segreti casuali protetti per ogni rilascio di Salesforce. L'HSM principale è separato dalla rete di produzione di Salesforce mediante "air gap" e archiviato in modo sicuro in una cassetta di sicurezza bancaria.

**Segreto master**

Utilizzato in associazione al segreto tenant e alla funzione di derivazione delle chiavi per generare una chiave di crittografia dei dati derivata. Il segreto master viene aggiornato a ogni rilascio da Salesforce e crittografato con la chiave di wrapping principale specifica di ogni rilascio, che a sua volta viene crittografata con la chiave pubblica dei server di derivazione delle chiavi in modo da poter essere archiviata crittografata nel file system. Solo gli HSM la possono decrittografare. *Nessun dipendente di Salesforce ha accesso a queste chiavi in formato testo normale.*

**Chiave di wrapping principale**

Una chiave simmetrica viene derivata e utilizzata come chiave di wrapping principale, nota anche come chiave master di wrapping, che crittografa tutto il bundle di chiavi e di segreti di ciascun rilascio.

**Segreto tenant**

Segreto specifico dell'organizzazione utilizzato in associazione al segreto master e alla funzione di derivazione delle chiavi per generare una chiave di crittografia dei dati derivata. Quando l'amministratore di un'organizzazione esegue la rotazione di una chiave, viene

generato un nuovo segreto tenant. Per accedere al segreto tenant tramite l'API, fare riferimento all'oggetto TenantSecret. *Nessun dipendente di Salesforce ha accesso a queste chiavi in formato testo normale.*

VEDERE ANCHE:

Torna all'argomento principale

Torna all'argomento principale

## Il processo di Crittografia piattaforma

Quando gli utenti inviano dei dati, il server di applicazioni cerca la chiave di crittografia dei dati specifica di quell'organizzazione all'interno della sua cache. Se la chiave non è presente, il server di applicazioni recupera il segreto tenant crittografato dal database, si autentica sul server di derivazione delle chiavi su un canale protetto e chiede al server di derivare la chiave. In seguito, il servizio di crittografia crittografa i dati sul server di applicazioni.

Salesforce genera in modo sicuro il segreto master e il segreto tenant mediante gli HSM (Hardware Security Modules). La chiave univoca viene derivata mediante PBKDF2, una funzione di derivazione delle chiavi (KDF), utilizzando il segreto master e il segreto tenant come input.

**Flusso del processo di Crittografia piattaforma**

1. I dati vengono inviati al server di applicazioni.
2. Il server di applicazioni cerca la chiave di crittografia dei dati specifica dell'organizzazione nella sua cache.
3. Se la chiave di crittografia dei dati non è presente nella cache:
    a. Il server di applicazioni recupera il segreto tenant crittografato dal database e chiede la chiave al server di derivazione delle chiavi.
    b. Il server di derivazione delle chiavi deriva la chiave nell'HSM servendosi del segreto master e del segreto tenant e la reinvia attraverso un canale protetto al server di applicazioni.
4. Il servizio di crittografia crittografa i dati sul server di applicazioni.
5. I dati crittografati vengono archiviati.

Salesforce genera un nuovo segreto master all'inizio di ciascun rilascio.

VEDERE ANCHE:

Torna all'argomento principale

Torna all'argomento principale

## Convalida automatica per Crittografia piattaforma

Quando si abilita la crittografia, Salesforce ne controlla automaticamente i potenziali effetti collaterali e avvisa qualora le impostazioni esistenti mettano a rischio l'accesso ai dati o il normale funzionamento dell'organizzazione Salesforce. Ad esempio, la crittografia viene bloccata se si tenta di crittografare dei campi utilizzati in regole di condivisione basate su criteri.

I risultati della convalida vengono inviati tramite email quando si utilizza l'interfaccia utente e sono sincroni quando si utilizza l'API.

Se quando si abilita Crittografia piattaforma il processo di convalida genera un messaggio di errore, le informazioni che seguono posso essere utili per risolvere il problema. Questi sono i fattori che vengono controllati dal servizio di convalida:

### Errori

| Se si utilizzano... | Soluzioni suggerite |
| --- | --- |
| Regole di condivisione basate sui criteri | Non è possibile utilizzare i campi nelle regole di condivisione basate sui criteri. |
| Query SOQL | I campi crittografati non si possono utilizzare in alcune parti di una query SOQL. |
| Campi formula | I campi formula non possono fare riferimento a campi crittografati. |
| Tabelle essenziali | I campi utilizzati nelle tabelle essenziali non si possono crittografare, e i campi crittografati non si possono utilizzare nelle tabelle essenziali. |
| Comunità e portali | Se si crittografano i campi standard non è possibile abilitare comunità o portali nell'organizzazione. Se comunità o portali sono già abilitati nell'organizzazione, i campi standard non si possono crittografare. |

**Nota:** le informazioni che seguono sono valide per Crittografia piattaforma e non per la crittografia classica.

VEDERE ANCHE:

Crittografia dei campi

Crittografia di file e allegati

Torna all'argomento principale

Crittografia dei campi

Crittografia di file e allegati

Torna all'argomento principale

## Autorizzazioni utente per Crittografia piattaforma

Per quanto riguarda la crittografia, assegnare le autorizzazioni agli utenti a seconda dei ruoli. Alcuni utenti avranno bisogno dell'autorizzazione "Visualizza dati crittografati", per altri saranno necessarie altre combinazioni di autorizzazioni per poter selezionare i dati da crittografare o utilizzare le chiavi di crittografia.

| | **Visualizza dati crittografati** | **Gestisci chiavi di crittografia** | **Personalizza applicazione** | **Visualizza impostazione e configurazione** |
|---|---|---|---|---|
| Visualizzare i dati nei campi crittografati | ✓ | | | |
| Visualizzare la pagina di impostazione di Crittografia piattaforma | | ✓ | ✓ | ✓ |
| Modificare la pagina di impostazione di Crittografia piattaforma escludendo la gestione delle chiavi | | | ✓ | |
| Visualizzare l'elenco dei segreti tenant | | ✓ | ✓ | ✓ |
| Generare, distruggere, esportare e importare i segreti tenant | | ✓ | | |

### L'autorizzazione "Visualizza dati crittografati"

È l'amministratore a decidere quali utenti possono vedere i valori dei campi senza mascheramento. A tale fine è necessario concedere l'autorizzazione "Visualizza dati crittografati" nei profili o negli insiemi di autorizzazioni. Gli amministratori non dispongono automaticamente di questa autorizzazione, e i profili standard non la prevedono per impostazione predefinita.

Suggerimento:

Quando si dispone dell'autorizzazione "Visualizza dati crittografati" e si concede l'accesso ad altri utenti, questi potranno visualizzare i valori dei campi crittografati sotto forma di testo normale. Per evitare di rendere visibili dati sensibili, clonare il proprio profilo, eliminare l'autorizzazione "Visualizza dati crittografati" dal profilo clonato e assegnare a se stessi il profilo clonato; a questo punto, concedere l'accesso all'altro utente.

Quando si concede o si revoca l'autorizzazione "Visualizza dati crittografati", gli utenti interessati ne vedono l'effetto solo dopo che il database è stato aggiornato.

Quando si attiva la crittografia, i valori presenti nei campi non vengono crittografati immediatamente, ma solo dopo essere stati modificati.

I file crittografati sono visibili a tutti gli utenti che hanno accesso ai file, indipendentemente dall'autorizzazione "Visualizza dati crittografati".

I valori dei campi crittografati sono senza maschera e possono essere visualizzati come testo normale per gli utenti che non dispongono dell'autorizzazione "Visualizza dati crittografati" nei seguenti casi:

- Trigger Apex
- Azioni
- Processi e funzioni eseguiti nel contesto di sistema

Gli utenti che non dispongono dell'autorizzazione "Visualizza dati crittografati" possono:

- Modificare il valore di un campo crittografato, a meno che la protezione a livello di campo non sia impostata su sola lettura.
- Visualizzare i campi crittografati nei risultati delle ricerche, anche se i valori saranno nascosti.

Gli utenti che non dispongono dell'autorizzazione "Visualizza dati crittografati" non possono:

- Modificare i campi di ricerca crittografati obbligatori.
- Utilizzare gli elenchi correlati del publisher Chatter.
- Utilizzare la funzionalità Copia indirizzo postale in altro indirizzo per i referenti.
- Scegliere quale valore conservare in due record account uniti se lo stesso valore è crittografato in entrambi. In questo caso, Salesforce conserva il valore del record account principale.

Quando l'utente in esecuzione di un rapporto o di un cruscotto digitale ha l'autorizzazione Visualizza dati crittografati, gli utenti che leggono i grafici del rapporto o il cruscotto digitale sprovvisti di questa autorizzazione potrebbero comunque vedere i dati crittografati.

Quando gli utenti sprovvisti di autorizzazione "Visualizza dati crittografati" clonano un record con campi non di ricerca crittografati, i valori dei campi crittografati appaiono vuoti nel nuovo record.

Quando un utente sprovvisto dell'autorizzazione "Visualizza dati crittografati" clona un record, i dati nei campi crittografati sono nascosti.

Nota: queste informazioni sono valide per Crittografia piattaforma e non per la crittografia classica.

VEDERE ANCHE:

Gestione dei segreti tenant e delle chiavi
Torna all'argomento principale
Gestione dei segreti tenant e delle chiavi
Torna all'argomento principale

## Crittografia piattaforma e distribuzione

Quando si distribuisce Crittografia piattaforma nell'organizzazione con IDE Force.com, lo strumento di migrazione o l'area di lavoro, l'attributo di campo Crittografato viene mantenuto. Se invece la distribuzione alle organizzazioni avviene con impostazioni di crittografia diverse, l'effetto dipende dall'abilitazione o meno di Crittografia piattaforma nell'organizzazione di destinazione.

Per distribuire Crittografia piattaforma ai campi personalizzati si possono utilizzare le serie di modifiche. Indipendentemente dalla modalità di distribuzione, Salesforce controlla automaticamente se l'implementazione viola le linee guida di Crittografia piattaforma.

Importante: i campi personalizzati nei pacchetti non si possono crittografare. Se nella distribuzione vengono utilizzati pacchetti gestiti o non gestiti, l'attributo di campo Crittografato viene ignorato.

| Organizzazione di origine | Organizzazione di destinazione | Risultato |
| --- | --- | --- |
| Crittografia piattaforma abilitata | Crittografia piattaforma abilitata | L'attributo di campo Crittografato di origine indica l'abilitazione |
| Crittografia piattaforma abilitata | Crittografia piattaforma non abilitata | L'attributo di campo Crittografato viene ignorato |
| Crittografia piattaforma non abilitata | Crittografia piattaforma abilitata | L'attributo di campo Crittografato di destinazione indica l'abilitazione |

EDIZIONI

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

Disponibile gratuitamente nella versione **Developer Edition** per le organizzazioni create a partire dal rilascio Summer '15.

**Nota:** le informazioni che seguono sono valide per Crittografia piattaforma e non per la crittografia classica.

VEDERE ANCHE:

Torna all'argomento principale
Torna all'argomento principale

## Crittografia piattaforma e Sandbox

L'aggiornamento di un Sandbox da un'organizzazione di produzione crea una copia esatta dell'organizzazione di produzione. Se nell'organizzazione di produzione è abilitato Crittografia piattaforma vengono copiate tutte le impostazioni di crittografia, compresi i segreti tenant creati nell'ambiente di produzione.

Dopo l'aggiornamento di un ambiente Sandbox, le modifiche del segreto tenant saranno disponibili solo nell'organizzazione corrente. In questo modo, in caso di rotazione o distruzione di un segreto tenant nell'organizzazione Sandbox, l'operazione non avrà alcun effetto sull'organizzazione di produzione.

Si consiglia di ruotare i segreti tenant negli ambienti Sandbox dopo aver eseguito l'aggiornamento. La rotazione garantisce che l'ambiente di produzione e l'ambiente Sandbox utilizzino segreti tenant diversi. La distruzione dei segreti tenant in un ambiente Sandbox rende inutilizzabili i dati crittografati nel caso di copie parziali o complete.

EDIZIONI

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

Disponibile gratuitamente nella versione **Developer Edition** per le organizzazioni create a partire dal rilascio Summer '15.

**Nota:** le informazioni che seguono sono valide per Crittografia piattaforma e non per la crittografia classica.

VEDERE ANCHE:

Torna all'argomento principale
Torna all'argomento principale

## Differenza tra crittografia classica e Crittografia piattaforma

La crittografia classica consente di proteggere un tipo speciale di campi di testo personalizzati, che vengono creati a questo scopo. Con Crittografia piattaforma è possibile crittografare molti campi standard di uso comune, oltre ad alcuni campi personalizzati e a numerosi tipi di file. Crittografia piattaforma supporta inoltre gli account personali, i casi, le ricerche, il flusso di lavoro, i processi di approvazione e altre funzioni essenziali di Salesforce.

| Funzione | Crittografia classica | Crittografia piattaforma |
|---|---|---|
| Prezzi | Inclusa nella licenza utente di base | Con supplemento di prezzo |
| Crittografia dati a riposo | ✓ | ✓ |
| Soluzione nativa (non richiede hardware né software) | ✓ | ✓ |
| Algoritmo di crittografia | AES (Advanced Encryption Standard) a 128 bit | AES (Advanced Encryption Standard) a 256 bit |
| Derivazione chiave basata su HSM | | ✓ |
| Autorizzazione "Gestisci chiavi di crittografia" | | ✓ |

| Funzione | Crittografia classica | Crittografia piattaforma |
| --- | --- | --- |
| Generazione, esportazione, importazione e distruzione chiavi | ✓ | ✓ |
| Conformità PCI-DSS L1 | ✓ | |
| Tipo campo di testo (crittografato) | Tipo di campo personalizzato dedicato, limitato a 175 caratteri | ✓ |
| Maschera | ✓ | ✓ |
| Tipi di maschera e caratteri | ✓ | |
| Autorizzazione "Visualizza dati crittografati" richiesta per la lettura dei valori dei campi crittografati | ✓ | ✓ |
| I valori del modello di email rispettano l'autorizzazione "Visualizza dati crittografati" | | ✓ |
| Campi standard crittografati | | ✓ |
| Allegati, file e contenuti crittografati | | ✓ |
| Campi personalizzati crittografati | | ✓ |
| Crittografia dei campi esistenti per tipi di campi personalizzati supportati | | ✓ |
| Ricerca (interfaccia utente, ricerca parziale, ricerche, alcune query SOSL) | | ✓ |
| Accesso API | ✓ | ✓ |
| Disponibile nelle regole di flusso di lavoro e negli aggiornamenti dei campi di flusso di lavoro | | ✓ |
| Disponibile nei criteri di immissione dei processi di approvazione e nei criteri delle fasi di approvazione | | ✓ |

VEDERE ANCHE:

Torna all'argomento principale

Torna all'argomento principale

# Considerazioni su Crittografia piattaforma

Crittografia piattaforma offre un'eccellente protezione dei dati. Tuttavia, prima di procedere alla sua attivazione, tenere presenti le seguenti considerazioni.

EDIZIONI

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**
Disponibile gratuitamente nella versione **Developer Edition** per le organizzazioni create a partire dal rilascio Summer '15.

IN QUESTA SEZIONE:



## Alcune applicazioni non funzionano con i dati crittografati

In alcuni gruppi di funzioni di Salesforce, l'uso dei dati crittografati a riposo non è supportato.

EDIZIONI

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**
Disponibile gratuitamente nella versione **Developer Edition** per le organizzazioni create a partire dal rilascio Summer '15.

Le applicazioni seguenti non supportano i dati crittografati a riposo. Consultare questa pagina per vedere le modifiche all'elenco delle applicazioni non supportate.

- Chatter Desktop
- Sistemi CTI (Computer-Telephony Integration)
- Connect Offline, Salesforce per Outlook, Exchange Sync e app Salesforce per Outlook
- Data.com
- ExactTarget
- Componenti Lightning
- Lightning Connect
- Live Agent
- Pardot
- Process Builder
- Salesforce Classic mobile
- Salesforce a Salesforce
- Site.com
- Visual Workflow
- Wave
- Work.com

Nota: queste informazioni sono valide per Crittografia piattaforma e non per la crittografia classica.

VEDERE ANCHE:

Torna all'argomento principale
Torna all'argomento principale

## Su alcuni campi, la crittografia ha conseguenze inattese

La crittografia di un determinato campo può avere effetti inattesi. Prima di decidere di crittografare un campo è bene sapere quale funzionalità sarà interessata.

EDIZIONI

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

Disponibile gratuitamente nella versione **Developer Edition** per le organizzazioni create a partire dal rilascio Summer '15.

Nota: le informazioni che seguono sono valide per Crittografia piattaforma e non per la crittografia classica.

| Campo | Oggetto | Effetto |
|---|---|---|
| Nome | Account | Exchange Sync restituisce un'eccezione quando sincronizza dati tra il server Microsoft Exchange dell'organizzazione e Salesforce. |
| Nome | Account | Non è possibile condividere account fra organizzazioni che utilizzano Salesforce a Salesforce. |
| Nome | Referente | I valori dei campi Titolo e Suffisso possono apparire nascosti agli utenti sprovvisti dell'autorizzazione "Visualizza dati crittografati" anche se i valori dei campi non sono crittografati. |
| Nome | Referente | Gli utenti sprovvisti di autorizzazione "Visualizza dati crittografati" possono creare record opportunità solo da azioni del publisher Chatter, elenchi correlati nelle pagine dei dettagli e Creazione rapida. |
| Nome | Qualsiasi | I campi di ricerca per l'oggetto sono di sola lettura. Non attiveranno regole di duplicazione durante il salvataggio di un record duplicato con un campo standard crittografato. |
| Email | Referente | Email a Salesforce non potrà ricevere messaggi email in entrata. |
| Email | Referente | Exchange Sync restituisce un'eccezione quando sincronizza dati tra il server Microsoft Exchange dell'organizzazione e Salesforce. |
| Campi personalizzati Email | Qualsiasi | I valori dei campi che contengono solo caratteri non ASCII sono limitati a 70 caratteri. Se si prevede che gli utenti immettano valori non ASCII, Salesforce consiglia di creare regole di convalida per imporre tali limiti. |
| Campi personalizzati Telefono | Qualsiasi | I valori dei campi che contengono solo caratteri non ASCII sono limitati a 22 caratteri. Se si prevede che gli utenti |

| Campo | Oggetto | Effetto |
| --- | --- | --- |
| | | immettano valori non ASCII, Salesforce consiglia di creare regole di convalida per imporre tali limiti. |

VEDERE ANCHE:


Crittografia dei campi

Torna all'argomento principale

Crittografia dei campi

Torna all'argomento principale


## Considerazioni generali su Crittografia piattaforma

EDIZIONI

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

Disponibile gratuitamente nella versione **Developer Edition** per le organizzazioni create a partire dal rilascio Summer '15.

Queste considerazioni sono valide per tutti i dati crittografati mediante Crittografia piattaforma.

**Ricerca**

- I file degli indici di ricerca non sono crittografati.
- Se si distrugge la chiave con cui sono stati crittografati dei campi, i termini di ricerca corrispondenti rimangono nell'indice di ricerca. Non è però possibile decrittografare i dati associati alla chiave distrutta.

**SOQL/SOSL**

- Se si eseguono query su dati crittografati, le stringhe non valide restituiscono un errore `INVALID_FIELD` anziché l'errore previsto `MALFORMED_QUERY`.
- I campi crittografati non possono essere utilizzati con le seguenti clausole e funzioni SOQL e SOSL:
  - Funzioni di aggregazione, ad esempio MAX(), MIN() e COUNT_DISTINCT()
  - Clausola WHERE
  - Clausola GROUP BY
  - Clausola ORDER BY
  - Query dinamiche all'interno di una classe Apex

Suggerimento: valutare se sostituire le clausole SOQL/WHERE con query SOSL/FIND.

**Account personali, account e referenti**

Quando si crittografano determinati campi in un account personale, vengono crittografati anche i campi equivalenti negli oggetti Account e Referente, e viceversa. Se alcuni campi account sono già stati crittografati e si abilitano gli account personali, vengono crittografati automaticamente i campi account personale appropriati. Questo vale per i campi seguenti:

- Nome account
- Nome referente
- Indirizzo postale
- Telefono
- Fax
- Cellulare
- Telefono abitazione

- Altro telefono
- Email

**Itinerario di controllo campi**

Se l'organizzazione ha abilitato l'itinerario di controllo campi, quando si attiva Crittografia piattaforma i dati archiviati in precedenza non vengono crittografati. Si immagini ad esempio che l'organizzazione usi l'itinerario di controllo campi per definire un criterio di conservazione della cronologia dei dati per un campo account come il campo del numero di telefono. Dopo avere abilitato Crittografia piattaforma si abilita la crittografia per quel campo e il numero di telefono dell'account viene crittografato. I record dei nuovi numeri di telefono vengono crittografati alla loro creazione, e i precedenti aggiornamenti del campo numero di telefono archiviati nell'elenco correlato Cronologia account vengono anch'essi crittografati. Invece, i dati cronologici relativi ai numeri di telefono già archiviati nell'oggetto `FieldHistoryArchive` continuano a restare senza crittografia. Se l'organizzazione ha l'esigenza di crittografare dei dati archiviati in precedenza, rivolgersi a Salesforce.

**Layout di pagina**

Se si visualizza l'anteprima di un layout di pagina come profilo senza autorizzazione "Visualizza dati crittografati", i dati di esempio dell'anteprima non saranno nascosti, ma risulteranno vuoti o saranno visualizzati come testo normale.

**Email**

- Se inclusi nei modelli di email, i valori dei campi crittografati appaiono come testo normale agli utenti con autorizzazione "Visualizza dati crittografati". In caso contrario, il destinatario vede i dati come testo normale o testo nascosto a seconda delle autorizzazioni degli utenti in esecuzione.
- Gli utenti sprovvisti dell'autorizzazione "Visualizza dati crittografati" non potranno inviare richieste Tieni i contatti.

**Cronologia attività**

Quando un elenco correlato Cronologia attività contiene riferimenti a campi crittografati, tali campi sono crittografati nel loro contesto originale e non nell'elenco correlato. L'elenco in sé non viene crittografato, e i valori non crittografati che contiene sono visibili come testo normale.

**API REST**

Se un campo è crittografato, non è possibile visualizzare i suggerimenti automatici tramite l'API REST.

**Importazione di dati**

Non è possibile utilizzare l'Importazione guidata dati per trovare corrispondenze utilizzando relazioni record principale-record dettaglio o aggiornare i record contenenti campi crittografati. La si può utilizzare invece per aggiungere nuovi record.

**Rapporti**

- I grafici dei rapporti e i componenti dei cruscotti digitali che visualizzano valori di campi crittografati si possono inserire nella cache su disco non crittografati.
- Non è possibile aggregare, ordinare o applicare filtri ai dati crittografati.

**generale**

- I campi crittografati non possono essere utilizzati in:
  - Regole di condivisione basate sui criteri
  - Criteri di filtro di visualizzazioni elenco, rapporti e cruscotti digitali
  - Portali: comunità, clienti, self-service e partner
  - Ricerche di opportunità simili
  - Relazioni di ricerca esterna
  - Tabelle essenziali
  - Criteri di filtro per gli strumenti di gestione dei dati

- Nell'app mobile Salesforce1, i dati dei campi crittografati dei record clonati dagli utenti sprovvisti dell'autorizzazione "Visualizza dati crittografati" sono nascosti.
- Gli utenti sprovvisti dell'autorizzazione "Visualizza dati crittografati" non potranno creare record che richiedono un valore per un campo standard crittografato.
- Gli utenti sprovvisti di autorizzazione "Visualizza dati crittografati" possono creare record referente e opportunità solo da azioni Chatter, elenchi correlati nelle pagine dei dettagli degli account e Creazione rapida.

Nota: le informazioni che seguono sono valide per Crittografia piattaforma e non per la crittografia classica.

VEDERE ANCHE:

Torna all'argomento principale

Torna all'argomento principale

# Protezione della sessione

Dopo l'accesso, un utente stabilisce una sessione con la piattaforma. Utilizzare la protezione della sessione per limitare l'esposizione alla rete quando un utente lascia incustodito il computer mentre è ancora connesso. In tal modo si limitano anche i rischi di attacchi interni, ad esempio quando un dipendente tenta di utilizzare la sessione di un collega.

È possibile controllare la finestra temporale di scadenza della sessione per gli accessi degli utenti. La scadenza della sessione consente di selezionare un timeout per le sessioni degli utenti. Il timeout della sessione predefinito è due ore di inattività. Allo scadere del timeout della sessione, viene visualizzata una finestra di dialogo che chiede agli utenti di disconnettersi o di continuare a lavorare. Se gli utenti non rispondono a questo messaggio, viene effettuata automaticamente la disconnessione.

Nota: Quando un utente chiude una finestra o una scheda del browser, non viene disconnesso automaticamente dalla sessione di Salesforce. Accertarsi che gli utenti siano consapevoli di questo e che terminino correttamente tutte le sessioni facendo clic su `Nome` > **Esci**.

Per impostazione predefinita, Salesforce utilizza TLS (Transport Layer Security) e richiede connessioni sicure (HTTPS) per tutte le comunicazioni. L'impostazione `Connessioni protette (HTTPS) richieste` determina se è necessario accedere a Salesforce tramite TLS (HTTPS), fatta eccezione per i siti Force.com a cui è comunque possibile accedere tramite HTTP. Se si chiede a Salesforce di disabilitare questa impostazione e modificare l'URL da `https://` a `http://` è comunque possibile effettuare l'accesso all'applicazione. Tuttavia, è necessario richiedere a tutte le sessioni di utilizzare TLS per aumentare la protezione. Vedere Modifica delle impostazioni di protezione della sessione a pagina 504.

È possibile limitare l'accesso ad alcuni tipi di risorse a seconda del livello di protezione associato al metodo di autenticazione (accesso) della sessione in corso dell'utente. Per impostazione predefinita, ciascun metodo di accesso può avere due diversi livelli di protezione: Standard o High Assurance. È possibile modificare il livello di protezione della sessione e definire criteri in modo da rendere disponibili risorse specifiche solo agli utenti con livello High Assurance. Per informazioni dettagliate, vedere Protezione a livello di sessione a pagina 507.

VEDERE ANCHE:

Impostazione degli intervalli IP affidabili per l'organizzazione

# Modifica delle impostazioni di protezione della sessione

È possibile modificare le impostazioni di protezione della sessione per specificare il tipo di connessione, le impostazioni del timeout e altro.

1. Da Imposta, immettere *Impostazioni di sessione* nella casella Ricerca veloce, quindi selezionare **Impostazioni di sessione**.
2. Personalizzare le impostazioni di protezione della sessione.

| Campo | Descrizione |
| --- | --- |
| Valore timeout | Periodo di tempo al termine del quale il sistema disconnette gli utenti inattivi. Per gli utenti del portale, il timeout è tra 10 minuti e 12 ore nonostante il valore minimo possa essere impostato solo su 15 minuti. Selezionare un valore compreso fra 15 minuti e 12 ore. Scegliere un valore di timeout più breve se l'organizzazione dispone di informazioni sensibili e si desidera adottare misure di sicurezza più severe.<br>Nota: Il valore temporale dell'ultima sessione attiva non viene aggiornato fino a metà del periodo di timeout. Perciò, con un timeout di 30 minuti, il sistema non verifica la presenza di attività finché non sono passati 15 minuti. Ad esempio, se si aggiorna un record dopo 10 minuti, il valore temporale dell'ultima sessione attiva non viene aggiornato perché non vi è stata attività dopo 15 minuti. L'utente viene disconnesso dopo altri 20 minuti (30 minuti in totale) perché il tempo dell'ultima sessione attiva non è stato aggiornato. Si supponga di aggiornare un record dopo 20 minuti, ossia 5 minuti dopo la verifica dell'ora dell'ultima sessione attiva. Il timeout viene azzerato e l'utente dispone di altri 30 minuti prima di essere disconnesso, per un totale di 50 minuti. |
| Disabilitare il popup di avviso del timeout di sessione | Determina se visualizzare un messaggio di avviso di timeout per gli utenti inattivi. Gli utenti vengono avvisati 30 secondi prima del timeout, come specificato da Valore timeout. |
| Forza disconnessione al timeout della sessione | Richiede che, quando le sessioni scadono per inattività degli utenti, le sessioni correnti non siano più valide. Il browser viene aggiornato e torna alla pagina di accesso. Per accedere all'organizzazione, l'utente deve eseguire nuovamente l'accesso. |

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

L'impostazione Bloccare le sessioni all'indirizzo IP da cui hanno avuto origine è disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Tutte le altre impostazioni disponibili nelle versioni: **Personal Edition**, **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni di protezione della sessione:

- "Personalizza applicazione"

| Campo | Descrizione |
| --- | --- |
| | Nota: *Non* selezionare `Disabilitare il popup di avviso del timeout sessione` quando si abilita questa opzione. |
| `Bloccare le sessioni all'indirizzo IP da cui hanno avuto origine` | Determina se bloccare le sessioni utente all'indirizzo IP da cui è stato effettuato l'accesso, in modo da impedire che persone non autorizzate accedano a una sessione valida.<br>Nota: Questa opzione può bloccare l'accesso di varie applicazioni e dispositivi mobili. |
| `Blocca le sessioni al dominio nel quale sono state utilizzate per la prima volta` | Associa una sessione dell'interfaccia utente corrente di un utente, ad esempio di un utente di comunità, con un dominio specifico per prevenire l'utilizzo non autorizzato dell'ID sessione in un altro dominio. Questa preferenza è abilitata per impostazione predefinita nelle organizzazioni create con il rilascio Spring '15 o successivi. |
| `Connessioni protette (HTTPS) richieste` | Indica se è necessario HTTPS per effettuare l'accesso a Salesforce, ad eccezione dei siti Force.com, cui si può ancora accedere mediante HTTP.<br>Per motivi di sicurezza, questa opzione è abilitata per impostazione predefinita.<br>Nota: La pagina Reimpostazione delle password per gli utenti è accessibile solo utilizzando HTTPS. |
| `Imponi nuovo accesso dopo accesso come utente` | Indica se un amministratore che ha eseguito l'accesso come un altro utente viene riportato alla sessione precedente dopo essersi disconnesso come utente secondario.<br>Se l'opzione è abilitata, un amministratore, dopo essersi disconnesso dalla sessione che aveva aperto come un altro utente, deve eseguire nuovamente l'accesso per continuare a utilizzare Salesforce; in caso contrario, viene riportato alla sua sessione originale. Questa opzione è abilitata per impostazione predefinita per le nuove organizzazioni a partire dal rilascio Summer '14. |
| `Richiedi attributo HttpOnly` | Limita l'accesso ai cookie degli ID sessione. Un cookie con l'attributo HttpOnly non è accessibile tramite metodi non HTTP, quali le chiamate da JavaScript.<br>Nota: Se si dispone di un'applicazione personalizzata o inserita in un pacchetto che utilizza JavaScript per accedere ai cookie degli ID sessione, selezionando `Richiedi attributo HttpOnly` si interrompe l'applicazione, poiché viene negato l'accesso al cookie da parte dell'applicazione. Se è selezionato `Richiedi attributo HttpOnly`, la finestra di debug del Toolkit AJAX non è disponibile. |
| `Utilizza le richieste POST per le sessioni tra domini diversi` | Stabilisce che l'organizzazione invii informazioni sulla sessione utilizzando una richiesta POST anziché una richiesta GET per gli scambi tra domini diversi, ad esempio quando un utente sta utilizzando una pagina Visualforce. In tale contesto, le richieste POST sono più sicure delle richieste GET, poiché le richieste POST mantengono le informazioni sulla sessione nel corpo della |

| Campo | Descrizione |
| --- | --- |
| | richiesta. Tuttavia, se si abilita questa impostazione, il contenuto incorporato da un altro dominio, ad esempio: `<img src="https://acme.force.com/pic.jpg"/>` potrebbe non essere visualizzato. |
| Imponi intervalli IP di accesso su ogni richiesta | Limita gli indirizzi IP dai quali gli utenti possono accedere a Salesforce ai soli indirizzi IP definiti in Intervalli IP di accesso. Se questa opzione è abilitata, gli intervalli IP di accesso vengono imposti su ogni richiesta di pagina, incluse le richieste provenienti dalle applicazioni client. Se questa opzione non è abilitata, gli intervalli IP di accesso vengono imposti solo quando un utente esegue l'accesso. Questa opzione riguarda tutti i profili con restrizioni IP di accesso. |
| Abilita caching e completamento automatico della password nella pagina di accesso | Consente al browser dell'utente di archiviare i nomi utente. Se abilitata, dopo che è stato effettuato un accesso iniziale, i nomi utente vengono compilati automaticamente nel campo Nome utente della pagina di accesso. Questa preferenza è selezionata per impostazione predefinita e sono abilitati il caching e il completamento automatico. |
| Abilita il metodo SMS di conferma dell'identità | Consente agli utenti di ricevere un PIN monouso consegnato via SMS. Se è selezionata questa opzione, gli amministratori o gli utenti devono verificare il loro numero di cellulare prima di utilizzare questa funzione. Questa impostazione è abilitata per impostazione predefinita in tutte le organizzazioni. |
| Richiedi token di protezione per gli accessi API dalle chiamate (versione API 31.0 e precedenti) | Richiede l'utilizzo dei token di protezione per gli accessi API da chiamate, ad esempio chiamate Apex o chiamate che utilizzano il proxy AJAX, in API versione 31.0 e precedenti. In API versione 32.0 e successive, i token di protezione sono richiesti per impostazione predefinita. |
| Intervalli IP di accesso (per le versioni Contact Manager Edition, Group Edition e Professional Edition) | Specifica un intervallo di indirizzi IP (compresi gli estremi) dal quale gli utenti devono effettuare l'accesso, in caso contrario l'accesso non riesce.<br>Per specificare un intervallo, fare clic su **Nuovo** e immettere un Indirizzo IP iniziale e un Indirizzo IP finale per definire l'intervallo, che include i valori di inizio e di fine.<br>Questo campo non è disponibile nelle versioni Enterprise Edition, Unlimited Edition, Performance Edition e Developer Edition. In queste versioni, è possibile specificare un intervallo IP di accesso valido nelle impostazioni del profilo utente. |
| Abilita la protezione dal clickjack per le pagine di impostazione | Protegge le pagine Salesforce di impostazione da attacchi clickjack. Il clickjacking consiste in un reindirizzamento del clic su di un altro oggetto. (Le pagine di impostazione sono disponibili dal menu Imposta.) |
| Abilitare la protezione dal clickjack per le pagine Salesforce non di impostazione | Protegge le pagine Salesforce non di impostazione da attacchi clickjack. Il clickjacking consiste in un reindirizzamento del clic su di un altro oggetto. Le pagine di impostazione prevedono già una protezione dal clickjack. (Le pagine di impostazione sono disponibili dal menu Imposta.) Questa impostazione è abilitata per impostazione predefinita in tutte le organizzazioni. |

| Campo | Descrizione |
| --- | --- |
| Abilita la protezione dal clickjack per le pagine Visualforce dei clienti con intestazioni standard | Protegge le pagine Visualforce con intestazioni abilitate da attacchi clickjack. Il clickjacking consiste in un reindirizzamento del clic su di un altro oggetto.<br>Avvertenza: se si utilizzano pagine Visualforce personalizzate all'interno di un frame o iframe, potrebbe apparire una pagina vuota o una pagina senza frame. Ad esempio, le pagine Visualforce in un layout di pagina non funzionano quando è attiva la protezione dal clickjack. |
| Abilita la protezione dal clickjack per le pagine Visualforce dei clienti con intestazioni disabilitate | Protegge le pagine Visualforce con intestazioni disabilitate da attacchi clickjack quando si imposta `showHeader="false"` sulla pagina. Il clickjacking consiste in un reindirizzamento del clic su di un altro oggetto.<br>Avvertenza: se si utilizzano pagine Visualforce personalizzate all'interno di un frame o iframe, potrebbe apparire una pagina vuota o una pagina senza frame. Ad esempio, le pagine Visualforce in un layout di pagina non funzionano quando è attiva la protezione dal clickjack. |
| Abilita la protezione dal CSRF sulle richieste GET per le pagine non di impostazione<br>Abilita la protezione dal CSRF sulle richieste POST per le pagine non di impostazione | Protegge dagli attacchi Cross Site Request Forgery (CSRF) modificando le pagine non di impostazione in modo che contengano una stringa di caratteri casuali nei parametri dell'URL o come campo modulo nascosto. Con ogni richiesta GET e POST, l'applicazione controlla la validità di questa stringa di caratteri ed esegue il comando solo se il valore trovato corrisponde a quello atteso. Questa impostazione è abilitata per impostazione predefinita in tutte le organizzazioni. |
| URL di disconnessione | Reindirizza gli utenti a una pagina specifica quando si disconnettono da Salesforce, ad esempio alla pagina di un provider di autenticazione o a una pagina con immagine aziendale personalizzata. Questo URL viene usato solo se non è specificato alcun URL di disconnessione nelle impostazioni del provider di identità, di Single Sign-On SAML o del provider di autenticazione esterno. Se per `URL di disconnessione` non viene specificato alcun valore, l'impostazione predefinita è `https://login.salesforce.com`, a meno che non sia abilitato Dominio personale. Se è abilitato Dominio personale, l'impostazione predefinita è `https://`*`dominiopersonale`*`.my.salesforce.com`. |

3. Fare clic su **Salva**.

## Livelli di sicurezza sessione

È possibile limitare l'accesso a certi tipi di risorse in base al livello di protezione associato al metodo di autenticazione (accesso) per la sessione corrente dell'utente. Per impostazione predefinita, ogni metodo di accesso ha due livelli di protezione: Standard o High Assurance. È possibile modificare il livello di protezione della sessione e definire le policy in modo che le risorse specificate siano disponibili solo per gli utenti con livello High Assurance.

Per impostazione predefinita, ai diversi metodi di autenticazione vengono assegnati questi livelli di protezione.

- Nome utente e password — Standard
- Autenticazione delegata — Standard
- Autenticazione a due fattori — High Assurance
- Provider di autenticazione — Standard
- SAML — Standard

  Nota: Il livello di protezione per una sessione SAML può essere specificato anche utilizzando l'attributo `SessionLevel` dell'asserzione SAML inviata dal provider di identità. L'attributo può utilizzare uno di due valori, `STANDARD` o `HIGH_ASSURANCE`.

Per modificare il livello di protezione associato a un metodo di accesso:

1. Da Imposta, immettere *Impostazioni di sessione* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni di sessione**.
2. Selezionare il metodo di accesso da Livelli di sicurezza sessione.
3. Fare clic sulla freccia **Aggiungi** o **Rimuovi** per spostarla nella categoria corretta.

Attualmente le uniche funzioni che utilizzano la protezione a livello di sessione sono rapporti e cruscotti digitali in Rapporti e cruscotti digitali Salesforce e le applicazioni connesse. È possibile impostare policy che richiedono High Assurance per questi tipi di risorsa e specificare un'azione da intraprendere se la sessione utilizzata per accedere alla risorsa non è High Assurance. Le azioni supportate sono:

- Blocca: l'accesso alla risorsa viene bloccato visualizzando un errore dovuto all'insufficienza di privilegi.
- Innalza livello sessione: reindirizza l'utente all'autenticazione completa a due fattori. Una volta completata correttamente l'autenticazione, l'utente può accedere alla risorsa. Per i rapporti e i cruscotti digitali, è possibile applicare questa azione quando gli utenti accedono ai rapporti o ai cruscotti digitali, oppure solo quando esportano e stampano i rapporti.

Avvertenza: l'innalzamento del livello di sessione su High Assurance tramite il reindirizzamento dell'utente all'autenticazione a due fattori non è un'azione supportata in Lightning Experience. Se nell'organizzazione è abilitato Lightning Experience e si imposta un criterio che richiede una sessione High Assurance per accedere a rapporti e cruscotti digitali, gli utenti Lightning Experience con una sessione Standard Assurance non possono accedere a rapporti e cruscotti digitali. Inoltre, non visualizzano le icone per queste risorse nel menu di navigazione. Per risolvere il problema, gli utenti che dispongono di una sessione Standard Assurance possono disconnettersi e poi riconnettersi utilizzando un metodo di autenticazione definito come High Assurance dalla loro organizzazione. Potranno quindi accedere a rapporti e cruscotti digitali. In alternativa, possono passare a Salesforce Classic, dove verrà loro richiesto di innalzare il livello di sessione quando tentano di accedere a rapporti e cruscotti digitali.

Per impostare una policy High Assurance richiesta per l'accesso a un'applicazione connessa:

1. Da Imposta, immettere *Applicazioni connesse* nella casella `Ricerca veloce`, quindi selezionare l'opzione per la gestione delle applicazioni connesse.
2. Fare clic su **Modifica** accanto all'applicazione connessa.
3. Selezionare **Richiesta sessione High Assurance**.
4. Selezionare una delle azioni presentate.
5. Fare clic su **Salva**.

Per impostare una policy High Assurance richiesta per l'accesso a rapporti e cruscotti digitali:

1. Da Imposta, immettere *Policy di accesso* nella casella `Ricerca veloce`, quindi selezionare **Policy di accesso**.
2. Selezionare **Richiesta sessione High Assurance**.
3. Selezionare una delle azioni presentate.
4. Fare clic su **Salva**.

I livelli di sessione non hanno alcun impatto sulle risorse dell'applicazione fatta eccezione per applicazioni connesse, rapporti e cruscotti digitali per i quali sono state definite policy di protezione esplicite.

VEDERE ANCHE:

Protezione della sessione

## Impostazione degli intervalli IP affidabili per l'organizzazione

Gli intervalli IP affidabili definiscono un elenco di indirizzi IP da cui gli utenti possono accedere senza ricevere una sollecitazione d'accesso per la verifica della loro identità, ad esempio un codice inviato al loro cellulare.

Per proteggere i dati della propria organizzazione da accessi non autorizzati, è possibile specificare un elenco di indirizzi IP dai quali gli utenti possono accedere senza ricevere una sollecitazione d'accesso. Tuttavia, questo non limita l'accesso in assoluto per gli utenti al di fuori dell'intervallo IP affidabile. Questi utenti possono infatti accedere dopo avere risposto alla sollecitazione d'accesso (in genere con l'inserimento di un codice inviato al loro dispositivo mobile o indirizzo email).

1. Da Imposta, immettere *Accesso di rete* nella casella `Ricerca veloce`, quindi selezionare **Accesso di rete**.
2. Fare clic su **Nuovo**.
3. Immettere un indirizzo IP valido nel campo `Indirizzo IP iniziale` e un indirizzo IP superiore nel campo `Indirizzo IP finale`.

   L'indirizzo iniziale e finale definiscono l'intervallo degli indirizzi IP da cui l'utente è autorizzato ad accedere, compresi i valori iniziale e finale. Se si desidera consentire l'accesso da un solo indirizzo IP, inserire lo stesso indirizzo in entrambi i campi. Ad esempio, per consentire l'accesso solo da 125.12.3.0, digitare 125.12.3.0 sia come indirizzo iniziale che come indirizzo finale.

   Il primo e l'ultimo indirizzo IP devono essere in un intervallo IPv4 e devono contenere al massimo 33.554.432 indirizzi ($2^{25}$, un blocco CIDR /7).

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

AUTORIZZAZIONI UTENTE

Per visualizzare l'accesso di rete:
- "Sollecitazione d'accesso abilitata"

Per modificare l'accesso di rete:
- "Gestisci indirizzi IP"

4. Se lo si desidera, immettere una descrizione per l'intervallo. Ad esempio, se si gestiscono più intervalli, immettere informazioni in merito all'area della rete a cui corrisponde questo intervallo.
5. Fare clic su **Salva**.

Nota: Per le organizzazioni attivate prima del dicembre 2007, Salesforce ha compilato automaticamente l'elenco degli indirizzi IP affidabili dell'organizzazione nel dicembre 2007, quando questa funzione è stata introdotta. A questi, sono stati aggiunti gli indirizzi IP da cui gli utenti affidabili avevano già avuto accesso a Salesforce nel corso dei sei mesi precedenti.

VEDERE ANCHE:

Protezione della sessione

Impostazione delle restrizioni di accesso

# Informazioni sulla sessione utente

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

La pagina Informazioni sessione utente consente di monitorare e proteggere la propria organizzazione visualizzando le sessioni attive e i relativi dettagli. È possibile creare visualizzazioni elenco personalizzate, visualizzare i dettagli di un utente associato a una sessione specifica e interrompere facilmente le sessioni sospette. Gli utenti non amministratori possono vedere le informazioni relative alla loro sessione, mentre gli amministratori possono vedere tutte le sessioni utente dell'organizzazione.

Quando si interrompe manualmente la sessione di un utente facendo clic sul pulsante **Rimuovi**, l'utente dovrà accedere nuovamente all'organizzazione.

La tabella che segue contiene informazioni sui campi visibili in questa pagina. Per via della natura della tecnologia di localizzazione geografica, la precisione dei campi di posizione geografica (ad esempio paese, città, codice postale) può variare.

| Campo | Descrizione |
|---|---|
| Città | Città in cui si trova fisicamente l'indirizzo IP dell'utente. Questo valore non è localizzato. |
| Paese | Paese in cui si trova fisicamente l'indirizzo IP dell'utente. Questo valore non è localizzato. |
| Codice paese | Codice ISO 3166 del paese in cui si trova fisicamente l'indirizzo IP dell'utente. Questo valore non è localizzato. Per ulteriori informazioni, vedere Codici paese - ISO 3166. |
| Creato | La data e l'indicazione oraria relative all'inizio della sessione. |
| Latitudine | Latitudine a cui si trova fisicamente l'indirizzo IP dell'utente. |
| Posizione | Posizione approssimativa dell'indirizzo IP da cui l'utente ha eseguito l'accesso. Per visualizzare ulteriori informazioni geografiche, ad esempio la città approssimativa e il codice postale, creare una visualizzazione personalizzata per includere tali campi. Questo valore non è localizzato. |
| Longitudine | Longitudine a cui si trova fisicamente l'indirizzo IP dell'utente. |
| Tipo di accesso | Il tipo di accesso associato alla sessione, ad esempio Applicazione, SAML e Portale. |
| ID sessione controllante | Se una sessione ha una sessione controllante, questo è l'ID univoco di tale sessione. |
| Codice postale | Codice postale in cui si trova fisicamente l'indirizzo IP dell'utente. Questo valore non è localizzato. |
| ID sessione | L'ID univoco della sessione. |
| Tipo di sessione | Tipo di sessione a cui l'utente ha eseguito l'accesso. Tra le più comuni, UI, Contenuto, API e Visualforce. |
| IP di origine | L'indirizzo IP associato alla sessione. |
| Suddivisione | Nome della suddivisione in cui si trova fisicamente l'indirizzo IP dell'utente. Questo valore non è localizzato. |
| Tipo di utente | Il tipo di profilo associato alla sessione. |
| Nome utente | Nome utente utilizzato per l'accesso alla sessione. Per visualizzare la pagina del profilo dell'utente, fare clic sul nome utente. |
| Aggiornati | Data e ora dell'ultimo aggiornamento della sessione in seguito a un'attività. Ad esempio, durante una sessione UI, gli utenti apportano spesso modifiche ai record e ad altri dati mentre lavorano. Con ogni modifica vengono aggiornate la data e l'indicazione oraria `Aggiornato` e `Valido fino a`. |

| Campo | Descrizione |
|---|---|
| Valido fino a | Se la sessione non viene interrotta manualmente, data e ora di scadenza automatica della sessione. |

VEDERE ANCHE:

Panoramica sull'autenticazione degli utenti

Tipi di sessione

## Tipi di sessione

Descrizione dei tipi di sessione nella pagina Informazioni sessione utente che consente di monitorare e proteggere l'organizzazione.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

La pagina Informazioni sessione utente consente di visualizzare il tipo di sessione per un determinato utente. Per accedere alla pagina, da Imposta immettere `Gestione sessione` nella casella `Ricerca veloce`, quindi selezionare **Gestione sessione**.

I tipi di sessione indicano il tipo di sessione utilizzata da un utente per accedere a un'organizzazione. I tipi di sessione possono essere permanenti o provvisori e accessibili mediante l'interfaccia utente, l'API o altri metodi, ad esempio un processo di autenticazione OAuth.

Nella seguente tabella sono descritti i tipi di sessione.

| Tipo di sessione | Descrizione |
|---|---|
| API | Creata quando si accede a un'organizzazione tramite API. |
| APIOnlyUser | Creata per abilitare la reimpostazione di una password nell'interfaccia utente per gli utenti solo API. |
| Chatter Networks | Creata quando si utilizzano Reti Chatter o Comunità Chatter. |
| ChatterNetworksAPIOnly | Creata quando si utilizzano API Reti Chatter o Comunità Chatter. |
| Content | Creata quando si rende disponibile contenuto caricato dall'utente. |
| OauthApprovalUI | Una sessione che consente solo l'accesso alla pagina di approvazione OAuth. |
| Oauth2 | Creata tramite flussi OAuth. Ad esempio, se si utilizza l'autenticazione OAuth per un'applicazione connessa, viene creato questo tipo di sessione. |
| SiteStudio | Creata quando si utilizza l'interfaccia utente Sites Studio. |
| SitePreview | Sessione che viene avviata quando viene richiamata un'applicazione area di disegno interna. Sarà sempre una sessione secondaria con una sessione principale interfaccia utente. |
| SubstituteUser | Sessione creata quando un utente esegue l'accesso tramite un altro utente. Ad esempio, se un amministratore accede come un altro utente, viene creata una sessione SubstituteUser. |
| TempContentExchange | Una sessione interfaccia utente provvisoria che consente di passare al dominio contenuti, ad esempio l'interfaccia utente in cui gli utenti digitano le proprie credenziali. |
| TempOauthAccessTokenFrontdoor | Una sessione provvisoria tramite il flusso di asserzioni token di accesso OAuth che non può essere aggiornata e deve essere mappata a un tipo di sessione regolare. |

| Tipo di sessione | Descrizione |
| --- | --- |
| TempVisualforceExchange | Una sessione provvisoria per passare al dominio Visuaforce. |
| TempUIFrontdoor | Una sessione provvisoria che non può essere aggiornata e deve essere mappata a un tipo di sessione regolare. |
| UI | Creata quando si utilizza una pagina dell'interfaccia utente. |
| UserSite | Avviata quando viene richiamata un'applicazione area di disegno. Si tratta sempre di una sessione secondaria con una sessione principale interfaccia utente. |
| Visualforce | Creata tramite una pagina Visualforce. |
| WDC_API | Una sessione che utilizza l'API Work.com. Si tratta sempre di una sessione secondaria e non può essere utilizzata nell'interfaccia utente. |

VEDERE ANCHE:

Panoramica sull'autenticazione degli utenti

Informazioni sulla sessione utente

# Attivazione della protezione

## Attivazioni con conferma dell'identità

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

Le attivazioni con conferma dell'identità tengono traccia delle informazioni sull'indirizzo IP del dispositivo attivato e sul browser client.

La conferma dell'identità serve per verificare le identità degli utenti provenienti da dispositivi sconosciuti e garantisce un ulteriore livello di protezione oltre all'autenticazione. All'utente proveniente da un dispositivo sconosciuto con un nuovo indirizzo IP viene richiesto di verificare la sua identità mediante il metodo di verifica con priorità più alta disponibile. In ordine di priorità, i metodi sono:

1. Codice di verifica generato da un'app di autenticazione mobile collegata all'account dell'utente.
2. Codice di verifica inviato tramite SMS al cellulare verificato dell'utente.
3. Codice di verifica inviato all'indirizzo email dell'utente.

Dopo che l'utente ha inserito il codice e completato la procedura di verifica dell'identità, il dispositivo (e il browser client) si considera attivato.

Nella pagina Attivazioni in Imposta gli amministratori e gli utenti finali di Salesforce possono vedere gli indirizzi IP dei dispositivi e i browser client attivati per un'organizzazione. Gli amministratori possono revocare lo stato di attivazione per la combinazione di dispositivo/browser di un determinato utente.

Per gli amministratori di Salesforce, la pagina Attivazioni in Imposta fornisce informazioni sugli indirizzi IP e i browser client di tutti i dispositivi attivati per tutti gli utenti dell'organizzazione. Gli amministratori possono revocare lo stato di attivazione di uno, di più utenti o di tutti gli utenti e possono filtrare le informazioni con criteri specifici quali il nome utente o l'indirizzo IP di accesso per decidere quali dispositivi attivati revocare.

Ad esempio, un utente può dire all'amministratore Salesforce che ha perso il dispositivo, ma che gliene è stato assegnato uno nuovo e che deve comunque poter accedere all'organizzazione. L'amministratore di Salesforce può revocare lo stato di attivazione del dispositivo

perso e del relativo browser client, eliminando di fatto i dati dell'indirizzo IP e del browser dal database. A chiunque tenti di accedere all'organizzazione da quel dispositivo revocato sarà chiesto di verificare la propria identità, aggiungendo un livello di protezione necessario e garantendo al tempo stesso la produttività degli utenti.

Per gli utenti, la pagina Attivazioni fornisce informazioni sugli indirizzi IP e sul browser client dei loro dispositivi attivati. Gli utenti finali possono revocare lo stato di attivazione solo per gli indirizzi IP e i browser client dei loro dispositivi attivati.

Ad esempio, un utente accede all'organizzazione e controlla i dispositivi attivati nella pagina Attivazioni, e nota che vi sono diversi dispositivi attivati. L'utente ha sempre eseguito l'accesso esclusivamente dal computer portatile dell'azienda e non riconosce gli indirizzi IP, per cui revoca immediatamente lo stato di attivazione di quei dispositivi. Poiché l'utente viene sollecitato a verificare la sua identità tramite un SMS sul suo dispositivo mobile, chiunque provi ad accedere all'organizzazione da uno dei dispositivi sconosciuti non sarà in grado di confermare la propria identità. L'utente a questo punto può segnalare la potenziale violazione della sicurezza.

VEDERE ANCHE:

Uso delle attivazioni con conferma dell'identità

## Uso delle attivazioni con conferma dell'identità

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

Le attivazioni con conferma dell'identità si usano per verificare e revocare lo stato di attivazione degli utenti.

Per vedere tutti gli IP di accesso e i browser attivati, da Imposta immettere *Attivazioni* nella casella Ricerca veloce, quindi selezionare **Attivazioni**. Gli indirizzi IP di accesso compaiono nella sezione IP di accesso attivato, mentre i browser sono visualizzati nella sezione Browser client attivati. Le voci meno recenti compaiono in cima agli elenchi.

Gli amministratori possono revocare lo stato di attivazione di uno o più utenti e indirizzi di dispositivi o di uno o più browser selezionando le voci corrispondenti, facendo clic su **Rimuovi** e confermando l'operazione. L'utente può visualizzare e revocare solo gli indirizzi IP e i browser attivati per il suo dispositivo. L'utente che è stato disattivato viene sollecitato a verificare la propria identità al successivo tentativo di accesso. Per attivare una verifica dell'identità è necessario revocare sia i dati dell'indirizzo IP di accesso, sia i dati del browser client.

È possibile creare visualizzazioni personalizzate degli indirizzi IP di accesso o dei browser client attivati facendo clic su **Crea nuova visualizzazione** e assegnando un nome alla visualizzazione, selezionando dei criteri di filtro e i campi da visualizzare e specificando la visibilità.

VEDERE ANCHE:

Attivazioni con conferma dell'identità

# Protezione degli utenti

## Panoramica sull'autenticazione degli utenti

Salesforce fornisce a ogni utente dell'organizzazione un nome utente e una password univoci che devono essere inseriti ogni volta che si effettua l'accesso. Salesforce genera un cookie della sessione per registrare le informazioni di autenticazione crittografate solo per la durata di una specifica sessione. Il cookie della sessione non include il nome utente né la password dell'utente. Salesforce non utilizza i

cookie per archiviare altre informazioni riservate dell'utente e della sessione, ma implementa metodi di sicurezza più avanzati basati sui dati dinamici e gli ID della sessione codificati.

VEDERE ANCHE:

Panoramica su Single Sign-On
Protezione a livello di rete
Protezione CAPTCHA per l'esportazione dati
Informazioni sulla sessione utente

## Panoramica su Single Sign-On

Salesforce possiede il proprio sistema di autenticazione degli utenti, ma alcune aziende preferiscono utilizzare una funzione Single sign-on esistente per semplificare e standardizzare l'autenticazione degli utenti. Sono disponibili due opzioni per implementare Single sign-on: l'autenticazione federata con SAML (Security Assertion Markup Language) o l'autenticazione delegata.

- L'autenticazione federata con SAML (Security Assertion Markup Language) consente di inviare i dati di autenticazione e autorizzazione tra servizi Web affiliati ma non correlati. In questo modo è possibile accedere a Salesforce da un'applicazione client. L'autenticazione federata con SAML è abilitata per impostazione predefinita per l'organizzazione.
- Il Single Sign-On con autenticazione delegata consente di integrare Salesforce con un metodo di autenticazione prescelto. Ciò permette di integrare l'autenticazione con il server LDAP (Lightweight Directory Access Protocol) o di eseguire l'accesso con Single sign-on effettuando l'autenticazione tramite un token anziché una password. L'autenticazione delegata viene gestita a livello di autorizzazione, consentendo ad alcuni utenti di utilizzare l'autenticazione delegata mentre altri continuano a utilizzare le loro password gestite da Salesforce. L'autenticazione delegata è impostata per autorizzazione e non a livello di organizzazione.

  I motivi principali per utilizzare l'autenticazione delegata comprendono:

  - Utilizzare un tipo di autenticazione utente più potente, quale l'integrazione con un provider d'identità sicuro
  - Rendere privata la pagina di accesso in modo che sia protetta dal firewall aziendale
  - Differenziare la propria organizzazione da tutte le altre società che utilizzano Salesforce per ridurre gli attacchi di phishing.

  È necessario richiedere che questa funzione sia abilitata da Salesforce. Per abilitare single sign-on mediante autenticazione delegata nella propria organizzazione, contattare Salesforce.
- I provider di autenticazione consentono agli utenti di accedere all'organizzazione Salesforce con le credenziali di accesso fornite da un provider di servizi esterno. Salesforce supporta il protocollo OpenId Connect che permette agli utenti di accedere da qualsiasi provider OpenID come Google, Paypal, LinkedIn e altri servizi che supportano OpenID Connect. Quando i provider di autenticazione sono abilitati, Salesforce non convalida la password dell'utente. Per definire le credenziali di autenticazione, Salesforce utilizza invece le credenziali di accesso dell'utente fornite da un provider di servizi esterno.

VEDERE ANCHE:

Panoramica sull'autenticazione degli utenti

## Protezione a livello di rete

L'autenticazione degli utenti determina chi può accedere, mentre la *protezione basata sulla rete* limita la provenienza e gli orari degli accessi. Utilizzare la protezione basata sulla rete per ridurre la finestra di opportunità disponibile agli autori degli attacchi limitando l'origine delle richieste di accesso degli utenti. La protezione basata sulla rete rende anche più difficile l'utilizzo delle credenziali rubate da parte degli autori degli attacchi.

Per ottimizzare la protezione basata sulla rete, è possibile limitare le ore in cui gli utenti possono accedere. Inoltre, è possibile limitare l'intervallo di indirizzi IP da cui gli utenti possono eseguire l'accesso a Salesforce. Se si definiscono delle restrizioni per gli indirizzi IP nel

profilo di un utente e viene eseguito un accesso da un indirizzo IP sconosciuto, Salesforce non consente l'accesso. Tali restrizioni consentono di proteggere i dati dagli accessi non autorizzati e dagli attacchi di phishing.

Per impostare l'elenco degli indirizzi IP affidabili dell'organizzazione dai quali gli utenti possono effettuare sempre l'accesso senza sollecitazione, vedere Impostazione degli intervalli IP affidabili per l'organizzazione a pagina 509. Per limitare gli orari di accesso in base al profilo o per limitare le richieste di accesso in base all'indirizzo IP per determinati profili, vedere Impostazione delle restrizioni di accesso a pagina 515.

VEDERE ANCHE:

Panoramica sull'autenticazione degli utenti

## Protezione CAPTCHA per l'esportazione dati

Su richiesta, Salesforce può anche chiedere agli utenti di superare un test di verifica per esportare i dati da Salesforce. Questo semplice test con immissione di testo impedisce ai programmi dannosi di accedere ai dati della propria organizzazione e di ridurre il rischio di attacchi automatizzati. CAPTCHA è un tipo di protezione basata sulla rete. Per superare il test, gli utenti devono digitare due parole visualizzate in una sovrapposizione all'interno della casella di testo della sovrapposizione e fare clic sul pulsante **Invia**. Salesforce utilizza la tecnologia CAPTCHA fornita da reCaptcha per verificare che un utente reale, e non un programma automatizzato, abbia inserito correttamente il testo nella sovrapposizione. CAPTCHA sta per "Completely Automated Public Turing Test To Tell Computers and Humans Apart" (ovvero "Test di Turing pubblico e completamente automatico per distinguere computer e umani").

VEDERE ANCHE:

Panoramica sull'autenticazione degli utenti

# Impostazione delle restrizioni di accesso

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

Per proteggere i dati dell'organizzazione dagli accessi non autorizzati, sono disponibili numerose opzioni di impostazione dell'accesso e delle restrizioni di accesso.

**Orari di accesso**

Per ogni profilo, è possibile impostare gli orari in cui gli utenti possono effettuare l'accesso. Vedere:

- Visualizzazione e modifica degli orari di accesso nell'interfaccia utente profilo ottimizzata
- Visualizzazione e modifica degli orari di accesso nell'interfaccia utente profilo originale

**Autenticazione a due fattori per accessi tramite interfaccia utente**

Per ogni profilo, è possibile chiedere agli utenti di immettere un token basato sul tempo come seconda forma di autenticazione quando accedono tramite l'interfaccia utente. Vedere Impostazione dei requisiti di accesso con autenticazione a due fattori a pagina 519.

**Autenticazione a due fattori per accessi tramite API**

Per ogni profilo, è possibile consentire l'uso di un token basato sul tempo anziché il token di protezione standard per accedere al servizio. Se gli utenti aggiungono un token basato sul tempo al proprio account e questa autorizzazione è abilitata, devono utilizzare questo token anziché il token di protezione standard ogni volta che viene richiesto, ad esempio per reimpostare la password dell'account. Vedere Impostazione dei requisiti dell'autenticazione a due fattori per l'accesso tramite API a pagina 520.

**Intervalli di indirizzi IP di accesso**

Per le versioni Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition e Database.com Edition, è possibile impostare gli indirizzi degli intervalli IP di accesso dai quali gli utenti possono effettuare l'accesso a un singolo profilo. Gli utenti all'esterno dell'intervallo IP di accesso impostato su un profilo non possono accedere all'organizzazione Salesforce. Vedere:

- Limitazione degli intervalli IP di accesso nell'interfaccia utente profilo ottimizzata
- Limitazione degli indirizzi IP di accesso nell'interfaccia utente profilo originale

Per le versioni Contact Manager Edition, Group Edition e Professional Edition, impostare l'intervallo IP di accesso. Da Imposta, immettere *Impostazioni di sessione* nella casella Ricerca veloce, quindi selezionare **Impostazioni di sessione**.

**Imposizione dell'intervallo di indirizzi IP di accesso per tutte le richieste di accesso**

È possibile limitare l'accesso globale a Salesforce agli indirizzi IP inclusi negli Intervalli IP di accesso nei profili utente. Si supponga ad esempio che un utente esegua correttamente l'accesso da un indirizzo IP definito negli Intervalli IP di accesso. In seguito, l'utente si sposta in un punto diverso e gli viene assegnato un nuovo indirizzo IP, che non rientra negli Intervalli IP di accesso. Quando l'utente aggiorna il browser o tenta di accedere a Salesforce, anche da un'applicazione client, l'accesso gli viene negato. Per abilitare questa opzione, da Imposta, immettere *Impostazioni di sessione* nella casella Ricerca veloce, selezionare **Impostazioni di sessione** e quindi **Imponi intervalli IP di accesso su ogni richiesta**. Questa opzione riguarda tutti i profili con restrizioni IP di accesso.

**Intervalli IP affidabili a livello dell'organizzazione**

È possibile impostare un elenco di intervalli di indirizzi IP dai quali tutti gli utenti possono eseguire l'accesso senza incorrere in alcun problema. Questi utenti potranno eseguire l'accesso all'organizzazione dopo aver fornito la verifica aggiuntiva. Vedere Impostazione degli intervalli IP affidabili per l'organizzazione.

Quando gli utenti accedono a Salesforce, mediante l'interfaccia utente, l'API, o un client desktop come Salesforce per Outlook, Connect Offline, Connect per Office o Data Loader, Salesforce verifica se l'accesso è autorizzato mediante la procedura seguente:

1. Salesforce controlla se al profilo dell'utente sono associate limitazioni di orario per l'accesso. In caso affermativo, qualsiasi tentativo di accesso eseguito al di fuori degli orari specificati viene respinto.
2. Se l'utente dispone dell'autorizzazione "Autenticazione a due fattori per gli accessi interfaccia utente", Salesforce richiede un token basato sul tempo (potrebbe anche chiedere all'utente di crearne uno se non lo ha già aggiunto all'account) al momento dell'accesso.
3. Se l'utente dispone dell'autorizzazione "Autenticazione a due fattori per gli accessi API" ed è stato aggiunto all'account un token basato sul tempo, Salesforce restituisce un errore se non viene utilizzato un token basato sul tempo anziché il token di protezione standard per accedere al servizio.
4. Successivamente, Salesforce controlla se al profilo dell'utente sono associate limitazioni relative all'indirizzo IP. In caso affermativo, qualsiasi tentativo di accesso eseguito da un indirizzo IP non specificato viene respinto, mentre sono consentiti gli accessi eseguiti da un indirizzo IP specificato. Se è abilitata l'impostazione di sessione **Imponi intervalli IP di accesso su ogni richiesta**, le limitazioni degli indirizzi IP vengono imposte per ogni richiesta di pagina, incluse le richieste provenienti dalle applicazioni client.
5. Se non sono impostate limitazioni dell'indirizzo IP in base al profilo, Salesforce controlla se l'utente sta eseguendo l'accesso da un indirizzo IP da cui non aveva mai eseguito l'accesso a Salesforce in precedenza:
   - Se l'utente accede da un browser che include un cookie Salesforce, l'accesso viene consentito. Se in precedenza l'utente ha utilizzato il browser per accedere a Salesforce e non ha cancellato i cookie, il browser dispone del cookie Salesforce.
   - Se l'utente accede da un indirizzo IP presente nell'elenco degli indirizzi IP affidabili dell'organizzazione, l'accesso viene consentito.
   - Se l'utente non accede né da un indirizzo IP affidabile né da un browser con un cookie Salesforce, l'accesso è bloccato.

Ogni volta che un tentativo di accesso viene bloccato o restituisce un errore di accesso API, Salesforce deve verificare l'identità dell'utente:

- Per accedere tramite interfaccia utente, viene richiesta l'immissione di un token (detto anche codice di verifica) per confermare l'identità dell'utente.

  Nota: al primo accesso a Salesforce non viene richiesto un codice di verifica.

- Per accedere tramite API o un client, l'utente deve aggiungere il proprio token di protezione (o token basato sul tempo se nel profilo dell'utente è impostata l'opzione Autenticazione a due fattori per gli accessi API e l'utente ha aggiunto un token basato sul tempo al proprio account) alla fine della password per poter eseguire l'accesso.

Un token di protezione è una chiave generata automaticamente da Salesforce. Ad esempio, se la password dell'utente è `passwordpersonale` e il token di protezione è `XXXXXXXXXX`, l'utente dovrà inserire `passwordpersonaleXXXXXXXXXX` per poter accedere. In alternativa, alcune applicazioni client dispongono di un campo separato per il token di protezione.

Gli utenti possono ricevere il proprio token di protezione modificando la password o reimpostando il token di protezione tramite l'interfaccia utente di Salesforce. Quando un utente modifica la password o reimposta il token di protezione, Salesforce invia un token di protezione all'indirizzo email del record Salesforce dell'utente. Il token di protezione è valido fino a quando l'utente non decide di reimpostarlo, di cambiare la password o di reimpostare la password.

Suggerimento: prima di accedere a Salesforce da un nuovo indirizzo IP, si consiglia di ottenere il proprio token di protezione da una rete affidabile utilizzando **Reimposta token di protezione personale**.

### Suggerimenti sull'impostazione delle restrizioni di accesso

Quando si impostano le limitazioni di accesso, prestare attenzione ai seguenti punti:

- Quando viene modificata la password di un utente, il token di protezione viene reimpostato. Finché l'utente non aggiunge, dopo la password, il token di protezione generato automaticamente quando accede a Salesforce tramite l'API o un client, l'accesso potrebbe essere bloccato.
- Agli utenti del Portale partner e del Portale Clienti non è richiesta l'attivazione del computer per accedere.
- Questi eventi vengono conteggiati ai fini del numero di tentativi di accesso che un utente può eseguire con una password non valida prima di essere bloccato da Salesforce, secondo quanto stabilito nelle impostazioni di blocco dell'accesso dell'organizzazione:
  - Ogni volta che agli utenti viene richiesto di confermare la loro identità (ad esempio, quando un utente seleziona **Inviami un codice di verifica per email**)
  - Ogni volta che gli utenti aggiungono il token di protezione o il token basato sul tempo in modo errato in fondo alla password per accedere all'API o a un client.

## Autenticazione a due fattori in Salesforce

Gli amministratori Salesforce possono ottimizzare la protezione richiedendo a ogni accesso un secondo livello di autenticazione detto "autenticazione a due fattori" (2FA). L'autenticazione a due fattori si può richiedere anche quando un utente soddisfa determinati criteri, ad esempio se tenta di visualizzare dei rapporti o di accedere da un indirizzo IP non riconosciuto.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

### Conferma di base dell'identità

Quando un utente esegue l'accesso, Salesforce ne esamina la posizione geografica e il browser. Se non li riconosce, Salesforce chiede all'utente di verificare la sua identità mediante il metodo di verifica con priorità più alta disponibile per quell'utente. L'ordine di priorità dei metodi di verifica è il seguente.

1. Codice di verifica generato da un'app di autenticazione mobile collegata all'account dell'utente.
2. Codice di verifica inviato tramite SMS al dispositivo mobile verificato dell'utente.
3. Codice di verifica inviato all'indirizzo email dell'utente.

L'utente immette il codice come verifica secondaria della propria identità. Dopo la verifica, non è necessario che l'utente fornisca di nuovo queste informazioni, a meno che l'accesso non avvenga da un browser o da una posizione che Salesforce non è in grado di verificare.

## Funzionamento dell'autenticazione a due fattori

Per un'ulteriore verifica dell'identità, è possibile richiedere un secondo livello di autenticazione a ogni accesso, a ogni accesso tramite API (per sviluppatori e applicazioni client) o per l'accesso a funzioni specifiche. L'autenticazione a due fattori utilizza un servizio di autenticazione, come l'app di autenticazione di Salesforce, l'app Google Authenticator o un altro servizio supportato. Il servizio fornisce un codice, detto TOTP (time-based one-time password) o "token basato sul tempo", che gli utenti specificano (oltre alla password) quando accedono.

Gli amministratori abilitano l'autenticazione a due fattori tramite le autorizzazioni. Gli utenti aggiungono l'app o il dispositivo di generazione di password singola del servizio di autenticazione tramite le impostazioni personali.

## Configurazione dell'autenticazione a due fattori

Gli amministratori Salesforce possono personalizzare le circostanze che richiedono agli utenti un secondo fattore di autenticazione nei seguenti modi.

- Richiedere l'autenticazione a ogni accesso. Impostare il requisito dell'accesso a due fattori per ogni accesso dell'utente a Salesforce. Questa funzione può essere abilitata anche per gli accessi API. Per ulteriori informazioni, vedere Impostazione dei requisiti di accesso con autenticazione a due fattori o Impostazione dei requisiti di autenticazione a due fattori per l'accesso tramite API.
- Utilizzare l'autenticazione "step-up" (nota anche come autenticazione "high assurance"). A volte non è necessario richiedere l'autenticazione a due fattori per ogni accesso degli utenti, ma si desidera proteggere determinate risorse. Se l'utente tenta di utilizzare un'applicazione connessa o di accedere a un rapporto, Salesforce gli chiede di inserire un codice di verifica. Per ulteriori informazioni, vedere Livelli di sicurezza sessione.
- Utilizzare i flussi di accesso. I flussi di accesso utilizzano Flow Designer e i profili per consentire la creazione di requisiti post autenticazione quando l'utente esegue l'accesso, inclusi i processi di autenticazione a due fattori. Per ulteriori informazioni, vedere gli esempi che seguono.
  - Flussi di accesso
  - Implementazione dell'autenticazione a due fattori basata su SMS
  - Enhancing Security with Two Factor Authentication

Gli utenti devono collegare un'app di autenticazione che genera il codice di verifica ai propri account Salesforce. Per ulteriori informazioni, vedere Connessione di un'app o di un dispositivo di generazione password singola.

VEDERE ANCHE:

Impostazione delle restrizioni di accesso

Flussi di accesso personalizzati

Eliminazione o ripristino dell'app generatore di password singole di un utente

## Impostazione dei requisiti di accesso con autenticazione a due fattori

Gli amministratori di Salesforce possono richiedere agli utenti che accedono a Salesforce di inserire una password a tempo da utilizzare una sola volta (TOTP) generata da un'app di autenticazione.

Per richiedere questa autenticazione ogni volta che gli utenti accedono a Salesforce, selezionare l'autorizzazione "Autenticazione a due fattori per gli accessi interfaccia utente" nel profilo o nell'insieme di autorizzazioni dell'utente.

Gli utenti devono inserire il codice generato dall'app di autenticazione ogni volta che accedono a Salesforce.

Una volta abilitata, l'autenticazione a due fattori sarà valida per gli utenti che accedono a Salesforce, comprese le organizzazioni con domini personalizzati creati con Dominio personale.

L'implementazione di base dell'autenticazione a due fattori non è valida per gli utenti dei seguenti metodi di autenticazione. È tuttavia possibile imporre l'autenticazione a due fattori per questi utenti utilizzando flussi di accesso personalizzati.

- SAML per Single Sign-On
- Social Sign-on in organizzazioni o Comunità.
- Autenticazione nome utente-password in Comunità.

VEDERE ANCHE:

Autenticazione a due fattori in Salesforce
Eliminazione o ripristino dell'app generatore di password singole di un utente
Flussi di accesso personalizzati

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Database.com Edition**, **Developer Edition**, **Enterprise Edition**, **Group Edition**, **Performance Edition**, **Professional Edition** e **Unlimited Edition**

AUTORIZZAZIONI UTENTE

Per modificare i profili e gli insiemi di autorizzazioni:

- "Gestisci profili e insiemi di autorizzazioni"

## Impostazione dei requisiti di autenticazione a due fattori per l'accesso tramite API

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Database.com Edition**, **Developer Edition**, **Enterprise Edition**, **Group Edition**, **Performance Edition**, **Professional Edition** e **Unlimited Edition**

AUTORIZZAZIONI UTENTE

Per modificare le autorizzazioni di sistema nei profili:

- "Gestisci profili e insiemi di autorizzazioni"

Per abilitare questa funzione:

- "Autenticazione a due fattori per accessi tramite interfaccia utente"

Gli amministratori di Salesforce possono impostare l'autorizzazione "Autenticazione a due fattori per gli accessi API" per consentire l'uso di una seconda autenticazione per l'accesso tramite API a Salesforce.

L'autorizzazione "Autenticazione a due fattori per accessi tramite interfaccia utente" è un prerequisito di "Autenticazione a due fattori per gli accessi API". Dopo aver abilitato queste autorizzazioni, gli utenti dovranno immettere un secondo valore di autenticazione quando accedono a Salesforce attraverso l'interfaccia utente. Questo secondo fattore di autenticazione è detto anche TOTP (time-based one-time password) o "token basato sul tempo".

Gli utenti possono collegare al proprio account un'app di autenticazione per generare la password a tempo da usare una sola volta.

VEDERE ANCHE:

Autenticazione a due fattori in Salesforce

Impostazione dei requisiti di accesso con autenticazione a due fattori

## Eliminazione o ripristino dell'app generatore di password singole di un utente

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

A un account utente può essere collegata una sola app mobile che genera password da usare una sola volta. Se l'utente non è più in grado di accedere all'app, ad esempio quando cambia o smarrisce il dispositivo mobile, l'app deve essere scollegata dall'account dell'utente. A questo punto, se lo si desidera è possibile collegare una nuova app.

La configurazione esistente dell'utente può essere rimossa dagli utenti e dagli amministratori Salesforce.

Nella pagina Dettagli utente avanzati, fare clic su **Disconnetti** in **Registrazione app: generatore di password singole**.

VEDERE ANCHE:

Visualizzazione e gestione degli utenti

## Flussi di accesso personalizzati

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

I flussi di accesso consentono agli amministratori di creare processi post-autenticazione adeguati alle procedure aziendali, di associare il flusso a un profilo utente e di inviare l'utente attraverso il flusso al momento dell'accesso. Utilizzare i flussi di accesso per raccogliere i dati di registrazione degli utenti, fornire un modulo di accettazione dei termini di servizio, richiedere all'utente un secondo fattore di autenticazione e altri tipi di personalizzazione.

Utilizzare Flow Designer per creare flussi di accesso e associarli quindi a profili specifici dell'organizzazione. È possibile connettere lo stesso flusso a più profili. Gli utenti con il profilo vengono indirizzati al flusso di accesso dopo l'autenticazione, ma prima di essere indirizzati ai contenuti dell'organizzazione. Le schermate del flusso di accesso vengono incorporate nella pagina di accesso standard di Salesforce per offrire all'utente un'esperienza di accesso integrata.

I flussi di accesso supportano tutti i metodi di autenticazione dell'interfaccia utente di Salesforce, compresi nome utente e password, autenticazione delegata, Single Sign-On SAML e accesso sociale tramite un provider di autenticazione esterno. I flussi di accesso si possono applicare alle organizzazioni, alle comunità e ai portali Salesforce.

Nota: i flussi di accesso non si possono applicare agli accessi API o quando le sessioni vengono passate all'interfaccia utente tramite `frontdoor.jsp` da un processo di accesso non da interfaccia utente. Sono supportati solo i flussi di tipo Flusso.

IN QUESTA SEZIONE:

Creazione di un flusso di accesso

Utilizzare Cloud Flow Designer per creare un processo per il flusso di accesso e quindi associare il flusso così ottenuto a un profilo.

Collegamento di un flusso di accesso a un profilo

Dopo avere creato un flusso di accesso in Flow Designer e averlo attivato è necessario associarlo a un profilo della propria organizzazione. Gli utenti con quel profilo vengono indirizzati al flusso di accesso.

## Creazione di un flusso di accesso

Utilizzare Cloud Flow Designer per creare un processo per il flusso di accesso e quindi associare il flusso così ottenuto a un profilo.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per aprire, modificare o creare un flusso in Cloud Flow Designer:
- "Gestisci Force.com Flow"

Quando il profilo di un utente è associato a un flusso di accesso, l'utente viene indirizzato al flusso nel corso del processo di autenticazione. Le schermate del flusso di accesso sono incorporate nella pagina di accesso standard di Salesforce. Durante il processo di autenticazione, a questi utenti viene limitato l'accesso alle schermate del flusso di accesso. Quando l'autenticazione va a buon fine e il flusso di accesso è completato, l'utente viene reindirizzato all'organizzazione. In caso contrario è possibile definire nel flusso un'azione esplicita per negare l'accesso.

Ad esempio, un amministratore può creare un flusso di accesso che implementa una procedura di autenticazione a due fattori personalizzata per aggiungere il livello di protezione desiderato. Un flusso di questo tipo utilizza metodi Apex per ottenere il contesto della sessione, estrarre l'indirizzo IP dell'utente e verificare se la richiesta proviene da un intervallo di indirizzi IP affidabili (per trovare o impostare l'intervallo di indirizzi IP affidabili, da Imposta immettere *`Accesso di rete`* nella casella `Ricerca veloce`, quindi selezionare **Accesso di rete**). Se la richiesta proviene da un intervallo di indirizzi IP affidabili, Salesforce salta il flusso e fa accedere l'utente all'organizzazione. In caso contrario, Salesforce invoca il flusso fornendo una delle tre opzioni seguenti.

1. Invita l'utente ad accedere con credenziali aggiuntive, ad esempio una password a tempo da usare una sola volta (TOTP, time-based one-time password).
2. Obbliga l'utente a disconnettersi.
3. Indirizza l'utente a una pagina con altre opzioni.

È possibile anche creare flussi di accesso che indirizzano gli utenti a pagine personalizzate quali moduli per raccogliere ulteriori informazioni o pagine che forniscono informazioni aggiuntive.

### Creazione del proprio flusso di accesso

Per crearsi un proprio flusso di accesso, seguire il procedimento descritto di seguito.

1. Creare un nuovo flusso con Flow Designer e Apex.

   Ad esempio, si può progettare un flusso di autenticazione a due fattori personalizzato basato sull'indirizzo IP che richiede un secondo fattore di autenticazione solo se l'utente accede da un indirizzo IP non compreso nell'intervallo degli indirizzi IP affidabili della rete aziendale (per trovare o impostare l'intervallo di indirizzi IP affidabili, da Imposta immettere *`Accesso di rete`* nella casella `Ricerca veloce`, quindi selezionare **Accesso di rete**).

   Nota: non impostare gli Intervalli IP di accesso direttamente nel profilo utente. Gli Intervalli IP di accesso impostati direttamente in un profilo limitano totalmente l'accesso all'organizzazione per gli utenti con quel profilo non compresi nell'intervallo, e questi utenti non possono entrare nel processo per il flusso di accesso.

   Il flusso deve contenere i seguenti elementi.

   a. Una nuova classe Apex che definisce un plugin Apex che viene implementato da (`Process.Plugin`) e utilizza la classe `Auth.SessionManagement` per accedere ai metodi e ai servizi della password a tempo da usare una sola volta (TOTP). La nuova classe Apex per il plugin genera una chiave a tempo con un codice di risposta rapida (QR) per convalidare la TOTP fornita dall'utente con la TOTP generata da Salesforce.

   b. Un elemento schermata per la scansione di un codice QR.

   c. Un elemento decisione che determini quando il token è valido e quando non lo è.

   All'interno del flusso è possibile impostare delle variabili di input. Se si usano i nomi specificati di seguito, all'avvio del flusso saranno compilati questi valori.

| Nome | Descrizione del valore |
| --- | --- |
| `LoginFlow_LoginType` | Il tipo di utente, ad esempio utente esterno comunità Chatter |
| `LoginFlow_IpAddress` | L'indirizzo IP attuale dell'utente. |
| `LoginFlow_LoginIpAddress` | L'indirizzo IP dell'utente utilizzato durante l'accesso, che può cambiare dopo l'autenticazione |
| `LoginFlow_UserAgent` | La stringa agente utente fornita dal browser dell'utente |
| `LoginFlow_Platform` | Il sistema operativo dell'utente |
| `LoginFlow_Application` | L'applicazione usata per richiedere l'autenticazione |
| `LoginFlow_Community` | La comunità corrente, se il flusso di accesso è valido per una comunità |
| `LoginFlow_SessionLevel` | Il livello di sicurezza sessione corrente, Standard o High Assurance |
| `LoginFlow_UserId` | L'ID utente di 18 caratteri. |

Durante il flusso è possibile assegnare i seguenti valori di variabili predefinite per un comportamento specifico.

Nota: il flusso carica questi valori solo *dopo* l'aggiornamento di una schermata dell'interfaccia utente (il clic di un utente su un pulsante non determina il caricamento dei valori: affinché questi siano caricati è necessario aggiungere una nuova schermata al flusso).

| Nome | Descrizione del valore |
| --- | --- |
| `LoginFlow_FinishLocation` | Valore di testo. Fornire una stringa che definisca la destinazione dell'utente una volta completato il flusso di accesso. La stringa deve essere un URL Salesforce valido (l'utente non può lasciare l'organizzazione e rimanere nel flusso) o un percorso relativo. |
| `LoginFlow_ForceLogout` | Valore booleano. Impostare questa variabile su `true` per disconnettere l'utente immediatamente e obbligarlo a uscire dal flusso. |

2. Salvare il flusso.
3. Attivare il flusso.
4. Collegare il flusso di accesso a un profilo.

VEDERE ANCHE:

Flussi di accesso personalizzati
https://developer.salesforce.com/page/Login-Flows
Collegamento di un flusso di accesso a un profilo

## Collegamento di un flusso di accesso a un profilo

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Dopo avere creato un flusso di accesso in Flow Designer e averlo attivato è necessario associarlo a un profilo della propria organizzazione. Gli utenti con quel profilo vengono indirizzati al flusso di accesso.

1. Da Imposta, immettere *Flussi di accesso* nella casella Ricerca veloce, quindi selezionare **Flussi di accesso**.
2. Fare clic su **Nuovo**.
3. Inserire un nome per fare riferimento all'associazione di quel flusso di accesso qualora sia necessario modificarla o eliminarla. Non è necessario che il nome sia univoco.
4. Selezionare il flusso di accesso per il profilo. L'elenco a discesa contiene tutti i flussi disponibili salvati in Flow Designer. Sono supportati solo i flussi attivi di tipo Flusso.
5. Selezionare una licenza utente per il profilo a cui si desidera collegare il flusso. L'elenco dei profili mostrerà i profili con quella licenza.
6. Selezionare il profilo da collegare al flusso di accesso.
7. Fare clic su **Salva**.

   Ora gli utenti del profilo saranno indirizzati al flusso di accesso impostato.

Dopo avere associato il flusso di accesso è possibile modificare o eliminare i flussi elencati in questa pagina dei flussi di accesso.

Un flusso di accesso si può associare a uno o più profili. mentre non è possibile collegare un profilo a più di un flusso di accesso.

VEDERE ANCHE:

Flussi di accesso personalizzati

Creazione di un flusso di accesso

# Policy sulla sicurezza delle transazioni

## Policy di sicurezza delle transazioni

EDIZIONI

Disponibile in: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**.

Le policy di sicurezza delle transazioni sono un modo per esaminare gli eventi dell'organizzazione e specificare le azioni da intraprendere quando si verificano determinate combinazioni di eventi. La sicurezza delle transazioni monitora gli eventi in base alle policy che sono state impostate. Quando viene attivata una policy è possibile scegliere di ricevere una notifica e, se lo si desidera, di eseguire un'azione.

Le policy valutano le attività utilizzando gli eventi specificati da chi le ha impostate. Per ogni policy si definiscono delle azioni in tempo reale come notifica, blocca, imponi l'autenticazione a due fattori o scegli una sessione da terminare. Quando si abilita la sicurezza delle transazioni per l'organizzazione vengono create una policy di limitazione delle sessioni simultanee e una classe Apex corrispondente. L'amministratore può abilitare subito la policy o modificare la classe Apex per personalizzarla.

Si immagini ad esempio di attivare la policy di limitazione delle sessioni simultanee per limitare il numero di sessioni simultanee per utente. Inoltre, si modifica la policy per ricevere un'email di notifica quando viene attivata la policy. Si aggiorna anche l'implementazione Apex della policy per limitare le sessioni utente a tre anziché alle cinque predefinite (è più semplice di quanto sembri). In seguito, un utente con tre sessioni di accesso tenta di crearne una quarta.

La policy glielo impedisce e lo obbliga a terminare una delle sessioni esistenti prima di avviare la nuova sessione. Contemporaneamente, l'amministratore riceve una notifica di attivazione della policy.

Una policy di sicurezza delle transazioni è costituita da eventi, notifiche e azioni.

- Policy valide per l'organizzazione, costituite da eventi. I tipi di eventi disponibili sono:
  - Esportazione di dati per gli oggetti Account, Referente, Lead e Opportunità
  - Entità per provider e sessioni di autenticazione, browser client e IP di accesso
  - Accessi
  - Accesso alla risorsa per applicazioni connesse, rapporti e cruscotti digitali
- Notifiche disponibili per la policy: la notifica può avvenire via email, all'interno di un'applicazione o in entrambi i modi.
- Azioni da intraprendere se viene attivata la policy:
  - Bloccare l'operazione
  - Richiedere un livello di sicurezza superiore con l'autenticazione a due fattori
  - Terminare una sessione in corso

  È anche possibile non intraprendere alcuna azione e ricevere solo una notifica. Le azioni disponibili dipendono dal tipo di evento selezionato.

## Configurazione della sicurezza delle transazioni

Prima di creare policy personalizzate è necessario attivare e configurare la sicurezza delle transazioni nella propria organizzazione. Questa funzione può essere utilizzata solo da un utente attivo cui è stato assegnato il profilo di amministratore di sistema.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**.

AUTORIZZAZIONI UTENTE

Per creare, modificare e gestire le policy di sicurezza delle transazioni:

- "Apex autore"

  E

  "Personalizza applicazione"

1. Prima di utilizzare le policy di sicurezza delle transazioni è necessario abilitarle. Questa operazione si esegue una sola volta, al primo accesso a Sicurezza delle transazioni.
   a. Da Imposta, immettere *`Sicurezza delle transazioni`* nella casella `Ricerca veloce`, quindi selezionare **Sicurezza delle transazioni**.
   b. Per abilitare la visualizzazione elenco delle policy e installare ConcurrentSessionsLimitingPolicy, selezionare **Abilita policy sulla sicurezza delle transazioni personalizzate** nella parte superiore della pagina.

   La policy ConcurrentSessionsLimitingPolicy limita le sessioni simultanee e viene attivata in due modi:

   - Quando un utente con cinque sessioni in corso tenta di accedere per aprire una sesta sessione.
   - Quando un amministratore che ha già eseguito l'accesso tenta di accedere una seconda volta.

   Il numero di sessioni ammesse si può cambiare modificando l'implementazione della policy Apex `ConcurrentSessionsPolicyCondition`.

2. Dopo avere abilitato la sicurezza delle transazioni, impostare le preferenze per l'organizzazione.
   a. Fare clic su **Preferenze predefinite** nella pagina Policy sulla sicurezza delle transazioni.
   b. Selezionare la preferenza **Quando gli utenti superano il numero massimo di sessioni Salesforce consentite, chiudi la sessione meno recente.**

Le policy di accesso influiscono sull'accesso a livello di programmazione e sull'accesso da Salesforce Classic e Lightning Experience. Quando si crea una policy che limita il numero di sessioni utente simultanee, tutte le sessioni contano ai fini di quel limite. Vengono considerati i normali accessi con nome utente e password, gli accessi da parte di applicazioni Web, gli accessi mediante provider di autenticazione e tutti gli altri tipi di accesso.

Il limite di sessioni non è un problema in Salesforce Classic o in Lightning Experience perché il sistema chiede di selezionare la o le sessioni da terminare. Questa scelta non è disponibile all'interno di un programma, per cui il programma visualizza un'eccezione di sicurezza delle transazioni per avvisare che è stato raggiunto il limite di sessioni consentite.

Selezionare la preferenza **Quando gli utenti superano il numero massimo di sessioni Salesforce consentite, chiudi la sessione meno recente** per evitare questo inconveniente. Quando a livello di programmazione viene fatta una richiesta che richiede un accesso ma non è consentita l'apertura di altre sessioni, le sessioni più vecchie vengono terminate fino a raggiungere un numero di sessioni attive inferiore al limite. L'impostazione è valida anche per gli accessi dall'interfaccia utente. Anziché chiedere di selezionare una sessione da terminare, il sistema termina automaticamente la sessione più vecchia e procede a effettuare l'accesso per la nuova sessione. Ecco come vengono gestite dai flussi OAuth le policy di accesso con e senza impostazione della preferenza.

| Tipo di flusso | Azione se è selezionata una preferenza | Azione se non è selezionata una preferenza |
|---|---|---|
| Server Web OAuth 2.0 | Codice di autorizzazione e token di accesso concessi<br>Le sessioni più vecchie vengono terminate fino a raggiungere un numero conforme alla policy. | Codice di autorizzazione concesso, token di autorizzazione no<br>Le sessioni più vecchie vengono terminate fino a raggiungere un numero conforme alla policy. |
| Utente-agente OAuth 2.0 | Token di accesso concesso<br>Le sessioni più vecchie vengono terminate fino a raggiungere un numero conforme alla policy. | Token di accesso concesso<br>Le sessioni più vecchie vengono terminate fino a raggiungere un numero conforme alla policy. |
| Flusso token di aggiornamento OAuth 2.0 | Token di accesso concesso<br>Le sessioni più vecchie vengono terminate fino a raggiungere un numero conforme alla policy. | Eccezione TXN_SECURITY_END_SESSION |
| Token bearer JWT OAuth 2.0 | Token di accesso concesso<br>Le sessioni più vecchie vengono terminate fino a raggiungere un numero conforme alla policy. | Eccezione TXN_SECURITY_END_SESSION |
| Asserzione bearer SAML OAuth 2.0 | Accesso concesso<br>Le sessioni più vecchie vengono terminate fino a raggiungere un numero conforme alla policy. | Eccezione TXN_SECURITY_END_SESSION |
| Nome utente e password OAuth 2.0 | Accesso concesso<br>Le sessioni più vecchie vengono terminate fino a raggiungere un numero conforme alla policy. | Accesso negato a causa di un numero di sessioni attive superiore a quello consentito dalla policy |
| Asserzione SAML | Non applicabile | Non applicabile |

Per ulteriori informazioni sui flussi di autenticazione, vedere Autenticazione delle applicazioni con OAuth nella Guida di Salesforce.

# Creazione di policy di sicurezza delle transazioni personalizzate

Creare delle policy personalizzate che vengono attivate da eventi specifici. Questa funzione può essere utilizzata solo da un utente attivo cui è stato assegnato il profilo di amministratore di sistema.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**.

AUTORIZZAZIONI UTENTE

Per creare, modificare e gestire le policy di sicurezza delle transazioni:
- "Apex autore"

  E

  "Personalizza applicazione"

1. Da Imposta, immettere *`Sicurezza delle transazioni`* nella casella `Ricerca veloce`, selezionare **Sicurezza delle transazioni** e fare clic su **Nuovo** in Policy sulla sicurezza delle transazioni personalizzate.
2. Compilare i campi con le informazioni di base per la nuova policy.
   - Per maggiore chiarezza e facilità di manutenzione, usare nomi simili per l'API e per la policy. Il nome può contenere solo caratteri di sottolineatura e alfanumerici e deve essere univoco nell'organizzazione. Deve iniziare con una lettera, non deve includere spazi, terminare con un carattere di sottolineatura, né contenere due caratteri di sottolineatura consecutivi.
   - `Tipo di evento` — Determina le azioni disponibili. Può essere uno dei seguenti:
     - **Accesso** — L'accesso di un utente. L'accesso consente di impostare qualsiasi combinazione di notifica, più le azioni seguenti:
       - Blocca completamente l'accesso
       - Richiedi l'autenticazione a due fattori per continuare
       - Richiedi la chiusura di una sessione di accesso in corso per continuare
     - **Entità** — Un tipo di oggetto. Selezionare una risorsa specifica e il tipo di notifiche desiderato.
     - **Esportazione dati** — Invia una notifica se il tipo di oggetto selezionato è stato esportato mediante il client API Data Loader.
     - **AccessResource** — Invia una notifica quando qualcuno accede alla risorsa selezionata. È possibile bloccare l'accesso o richiedere l'autenticazione a due fattori per concedere l'accesso.
   - `Notifiche` — È possibile selezionare tutti i metodi di notifica, alcuni metodi o nessun metodo per ogni policy.
   - `Destinatario` — Deve essere un utente attivo a cui è stato assegnato il profilo Amministratore di sistema.
   - `Azioni in tempo reale` — Specifica l'azione da eseguire quando viene attivata la policy. Le azioni disponibili variano a seconda del tipo di evento. Le notifiche via email e all'interno dell'applicazione sono sempre disponibili. Per gli eventi accesso e risorsa è possibile anche bloccare l'azione o richiedere un livello di controllo degli accessi più elevato con l'autenticazione a due fattori. Per gli eventi di accesso è possibile richiedere la conclusione di una sessione in corso prima di proseguire nella sessione corrente. È possibile impostare l'azione predefinita per terminare una sessione in modo che chiuda sempre la sessione più vecchia.

     Nota: in Salesforce1, l'autenticazione a due fattori per il tipo di evento AccessResource non è disponibile. Al suo posto viene utilizzata l'azione Blocca.

     Importante: non creare una policy che richiede l'autenticazione a due fattori senza prima fornire agli utenti un modo per procurarsi una password a tempo da utilizzare una sola volta. Questa password è il loro secondo fattore di autenticazione. In caso contrario, un utente che si trovi in una situazione che richiede un secondo fattore di autenticazione non potrà completare la sua operazione, ad esempio eseguire l'accesso o eseguire un rapporto.
   - È possibile utilizzare una classe esistente per `Policy Apex` o selezionare **Genera Apex** per creare una classe di policy predefinita che implementi l'interfaccia `TxnSecurity.PolicyCondition`.
   - L'utente selezionato per `Esegui policy come` deve avere il profilo di amministratore di sistema.

3. Se lo si desidera si può creare una condizione per una proprietà specifica nell'ambito della policy. Ad esempio, si può creare una policy che viene attivata quando qualcuno accede a un rapporto o a un cruscotto digitale da un indirizzo IP di origine specifico. L'indirizzo IP di origine è la proprietà che viene controllata.
   - Le proprietà disponibili dipendono dal tipo di evento selezionato.
   - Se il tipo di evento è Accesso è possibile cercare le modifiche alla proprietà verificatesi nell'arco di un determinato numero di giorni o una corrispondenza esatta del valore di una proprietà.
4. Per abilitare una policy, selezionare la casella di controllo corrispondente. Le policy si possono abilitare e disabilitare in funzione delle proprie esigenze.
5. Fare clic su **Salva**.

Dopo che i valori selezionati sono stati salvati, il sistema visualizza la pagina di modifica della nuova policy in cui si può modificare la policy ed esaminarne la classe Apex.

Se non si è specificato il valore di una condizione prima di generare l'interfaccia Apex per una policy, è possibile aggiungere la condizione in seguito. Modificare Apex code per includere una condizione prima di attivare la policy. Se non si include mai una condizione, la policy non sarà mai attivata. Alcuni esempi sono riportati in Policy Apex per le notifiche di sicurezza delle transazioni.

Si possono creare più policy per lo stesso tipo di evento, ma si consiglia di evitare la sovrapposizione delle policy e delle azioni corrispondenti. Tutte le policy per un determinato evento vengono attivate quando si verifica l'evento, ma l'ordine di attivazione non è definito. Ad esempio, se sono abilitate due policy per l'esportazione di un referente, non si può sapere quale delle due sarà attivata per prima. Se una policy copia il referente e l'altra lo elimina, l'operazione di copia non riuscirà se l'eliminazione ha già avuto luogo.

## Policy Apex per le notifiche di sicurezza delle transazioni

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**.

Ogni policy di sicurezza delle transazioni deve implementare l'interfaccia Apex `TxnSecurity.PolicyCondition`. Ecco alcuni esempi.

Se non si è specificato il valore di una condizione prima di generare l'interfaccia Apex per una policy, è possibile aggiungere la condizione in seguito. Modificare Apex code per includere una condizione prima di attivare la policy. Se non si include mai una condizione, la policy non sarà mai attivata. Per informazioni su come scrivere la condizione, vedere gli esempi che seguono.

L'implementazione `ConcurrentSessionsPolicyCondition` non viene eliminata quando si elimina una policy di sicurezza delle transazioni. L'Apex code si può riutilizzare in altre policy.

Questo esempio di policy Apex implementa una policy che viene attivata quando qualcuno ha eseguito un accesso da più indirizzi IP nell'arco delle ultime 24 ore.

Esempio:

```
global class LoginPolicyCondition implements
TxnSecurity.PolicyCondition {

 public boolean evaluate(TxnSecurity.Event e) {
 AggregateResult[] results = [SELECT SourceIp FROM LoginHistory
 WHERE UserId = :e.userId AND LoginTime = LAST_N_DAYS:1 GROUP
 BY SourceIp];

 if(!results.isEmpty() && results.size() > 1) {
  return true;
 }

 return false;
```

```
  }
}
```

Questo esempio di policy Apex implementa una policy che viene attivata quando si crea una sessione da un indirizzo IP specifico.

Esempio:

```
global class SessionPolicyCondition implements TxnSecurity.PolicyCondition {

 public boolean evaluate(TxnSecurity.Event e) {
 AuthSession eObj = [SELECT SourceIp FROM AuthSession WHERE Id = :e.entityId];
 if(eObj.SourceIp == '1.1.1.1' ){
  return true;
 }

 return false;
 }
}
```

Questa policy DataExport implementa una policy che viene attivata quando qualcuno esporta dati mediante Data Loader.

Esempio:

```
global class DataExportPolicyCondition implements TxnSecurity.PolicyCondition {

 public boolean evaluate(TxnSecurity.Event e) {
 if(e.data.get('SourceIp') == '1.1.1.1' ){
  return true;
 }

 return false;
 }
}
```

Questa policy Apex viene attivata quando qualcuno accede ai rapporti.

Esempio:

```
global class ReportsPolicyCondition implements TxnSecurity.PolicyCondition {

 public boolean evaluate(TxnSecurity.Event e) {
 if(e.data.get('SessionLevel') == 'STANDARD' ){
  return true;
 }

 return false;
 }
}
```

Questa policy Apex viene attivata quando qualcuno accede a un'applicazione connessa.

Esempio:

```
global class ConnectedAppsPolicyCondition implements TxnSecurity.PolicyCondition {

 public boolean evaluate(TxnSecurity.Event e) {
```

```
 if(e.data.get('SessionLevel') == 'STANDARD' && (e.entityId == '0CiD00000004Cce')){
  return true;
 }

 return false;
 }
}
```

## Gestione delle policy di sicurezza delle transazioni

Le policy di sicurezza delle transazioni servono per definire, abilitare e generare l'Apex code per implementare le policy. Specificare le modalità di notifica quando viene attivata una policy e quindi selezionare le policy da abilitare. Questa funzione può essere utilizzata solo da un utente attivo cui è stato assegnato il profilo di amministratore di sistema.

1. Da Imposta, immettere *`Sicurezza delle transazioni`* nella casella `Ricerca veloce`, quindi selezionare **Sicurezza delle transazioni**.
2. Dalla pagina Policy sulla sicurezza delle transazioni è possibile:
   - Modificare una visualizzazione
   - Creare una visualizzazione
   - Modificare una policy
   - Creare una policy
   - Modificare la classe Apex `TxnSecurity.PolicyCondition` di una policy
   - Eliminare una policy
   - Impostare le preferenze predefinite per la sicurezza delle transazioni.

Le preferenze predefinite di sicurezza delle transazioni si possono modificare in qualsiasi momento.

EDIZIONI

Disponibile in: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**.

AUTORIZZAZIONI UTENTE

Per creare, modificare e gestire le policy di sicurezza delle transazioni:
- "Apex autore"

  E

  "Personalizza applicazione"

## Ricezione delle notifiche relative alla sicurezza delle transazioni

Le notifiche selezionate si ricevono quando viene attivata una policy abilitata. Le notifiche sono formattate per essere facilmente riconoscibili.

EDIZIONI

Disponibile in: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**.

### Notifiche per email

Le notifiche per email vengono inviate da Sicurezza delle transazioni con l'oggetto "Avviso sulla sicurezza delle transazioni!". Il corpo del messaggio contiene la policy che è stata attivata e l'evento o gli eventi che l'hanno attivata. Gli orari riportati si riferiscono al momento in cui è stata attivata la policy secondo le impostazioni internazionali e il fuso orario del destinatario. Si immagini ad esempio che una policy venga attivata alle 18:46 nel fuso orario Eastern Standard Time. Il fuso orario dell'amministratore che riceve la notifica è Pacific Standard Time, per cui gli orari sono visualizzati secondo il fuso orario PST. Ecco un esempio.

Esempio:

```
From: Transaction Security <noreply@salesforce.com>
To: Admin@company.com
Sent: Friday, November 12, 2014, 5:35 PM
Subject: Transaction Security Alert!

This is a transaction security policy alert.

Policy: An administrator created a new user.

Event(s) responsible for triggering this policy:
1. Created new user Lisa Johnson at 11/12/2014 5:35:09 PM PST
```

### Notifiche all'interno dell'applicazione

Le notifiche all'interno dell'applicazione sono disponibili solo per gli utenti di Salesforce1. La notifica mostra la policy che è stata attivata. Ecco un esempio.

Esempio:

```
Transaction Security Alert:
Policy New Encrypted Custom Field was triggered.
```

# Dominio personale

## Panoramica su Dominio personale

Potenziare la protezione dell'accesso e aggiungere l'immagine aziendale alle pagine della propria organizzazione abilitando il dominio personalizzato.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Performance Edition**, **Unlimited Edition**, **Enterprise Edition**, **Developer Edition**, **Professional Edition** e **Group Edition**.

Utilizzando Dominio personale, è possibile definire un nome di dominio Salesforce personalizzato. Il nome di dominio personalizzato aiuta a gestire al meglio l'accesso e l'autenticazione per l'organizzazione in diversi modi.

- Dare risalto all'identità della propria attività con l'URL del dominio univoco.
- Aggiungere l'immagine aziendale alla schermata di accesso e personalizzare il contenuto del frame destro.
- Bloccare o reindirizzare le richieste di pagine che non utilizzano il nuovo nome di dominio.
- Accedere a un maggior supporto per Single Sign-On. Dominio personale deve utilizzare alcune funzioni di Identity di Salesforce, ad esempio i provider di autenticazione e i provider di identità.
- Impostare una policy di accesso personalizzata e stabilire in che modo gli utenti vengono autenticati.
- Consentire agli utenti di selezionare un provider di identità alternativo dalla pagina di accesso.

È possibile definire un nome di dominio personalizzato una sola volta. Dominio personale è disponibile anche per gli ambienti Sandbox.

Nota: Dominio personale è soggetto a Condizioni di utilizzo aggiuntive.

Il nome di dominio utilizza il formato URL standard, che comprende:

- Il protocollo: https://
- Il prefisso di sottodominio: il proprio marchio o termine
- Il dominio: my.salesforce.com

Ad esempio, una società denominata Universal Containers vuole utilizzare il sottodominio `universalecontainers`. L'URL di accesso della società sarebbe `https://universalcontainers.my.salesforce.com/`. È possibile utilizzare fino a 40 caratteri.

Salesforce è abilitato automaticamente come provider di identità quando viene creato un dominio. Dopo che il dominio è stato distribuito, è possibile aggiungere o modificare i provider di identità e incrementare la protezione dell'organizzazione personalizzando la policy di accesso del dominio.

**Importante:** Una volta distribuito il nuovo nome di dominio, non sarà più possibile annullarne la distribuzione.

VEDERE ANCHE:

Impostazione di un nome di dominio

Modifiche dell'URL del Dominio personale

Verifica e distribuzione del nuovo nome di dominio

Linee guida e procedure consigliate per l'implementazione del dominio personale

Ottenere informazioni sulle prestazioni e la manutenzione del sistema tramite Dominio personale

## Impostazione di un nome di dominio

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Performance Edition**, **Unlimited Edition**, **Enterprise Edition**, **Developer Edition**, **Professional Edition** e **Group Edition**.

AUTORIZZAZIONI UTENTE

Per impostare un nome di dominio:

- "Personalizza applicazione"

L'implementazione del nome di dominio personalizzato è rapida e semplice.

1. Trovare un nome di dominio disponibile e registrarsi per utilizzarlo.
2. Personalizzare il logo, lo sfondo e il contenuto del frame destro della pagina di accesso.
3. Aggiungere o modificare i provider di identità disponibili sulla pagina di accesso.
4. Verificare il nome di dominio e distribuirlo a tutta l'organizzazione.
5. Impostare la policy di accesso per gli utenti che accedono alle pagine.

VEDERE ANCHE:

Panoramica su Dominio personale

Definizione del nome di dominio

Verifica e distribuzione del nuovo nome di dominio

Impostazione della policy di accesso del dominio personale

Personalizzazione dell'immagine aziendale della pagina di accesso

Aggiunta di provider di identità a una pagina di accesso

## Definizione del nome di dominio

Registrarsi per il nome di dominio personalizzato per la propria organizzazione.

Per iniziare a impostare il nome di dominio personalizzato, trovare un nome dominio univoco per la propria organizzazione e registrarsi.

1. Da Imposta, digitare *`Dominio personale`* nella casella `Ricerca veloce` e quindi selezionare **Dominio personale**.
2. Immettere il nome del sottodominio che si desidera utilizzare nell'URL di esempio. Ad esempio, una società denominata Universal Containers vuole utilizzare il sottodominio `universalecontainers`. L'URL di accesso della società sarebbe `https://universalcontainers.my.salesforce.com/`. È possibile utilizzare fino a 40 caratteri.

   Per sicurezza, non è possibile utilizzare queste parole riservate per i sottodomini:

   - www
   - salesforce
   - heroku

   E il nome del dominio non può iniziare con queste parole:

   - root
   - status
3. Fare clic su **Verifica disponibilità**. Se il nome è già utilizzato, sceglierne uno diverso.
4. Fare clic su **Termini e condizioni** per rivedere l'accordo, quindi selezionare la casella di controllo.
5. Fare clic su **Registra dominio**.
6. Non appena il nome di dominio è pronto per i test, verrà inviato un messaggio email. (Possono essere necessari da 30 secondi a 24 ore.)

Il dominio non viene diffuso fino a che non è stato testato e distribuito.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Performance Edition**, **Unlimited Edition**, **Enterprise Edition**, **Developer Edition**, **Professional Edition** e **Group Edition**.

AUTORIZZAZIONI UTENTE

Per definire un nome di dominio:

- "Personalizza applicazione"

VEDERE ANCHE:

Impostazione di un nome di dominio
Linee guida e procedure consigliate per l'implementazione del dominio personale
Modifiche dell'URL del Dominio personale
Verifica e distribuzione del nuovo nome di dominio

## Linee guida e procedure consigliate per l'implementazione del dominio personale

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Performance Edition**, **Unlimited Edition**, **Enterprise Edition**, **Developer Edition**, **Professional Edition** e **Group Edition**.

Questi suggerimenti agevolano la transizione a un nuovo nome di dominio.

- Eseguire prima una prova nel Sandbox, poiché non è possibile impostare le policy di accesso prima di distribuire il dominio. Per verificare queste personalizzazioni, funzionalità personalizzate dell'interfaccia utente, pagine Visualforce e modiche di URL delle applicazioni, definire e distribuire un nome di dominio in un ambiente Sandbox.
- Distribuire il nuovo dominio quando l'organizzazione riceve un traffico molto limitato, ad esempio durante il fine settimana, in modo da risolvere eventuali problemi quando il traffico non influisce.
- Se si è deciso di personalizzare l'interfaccia utente di Salesforce con funzionalità quali pulsanti personalizzati o pagine Visualforce, effettuare una verifica degli elementi personalizzati prima di distribuire il nome di dominio. Le personalizzazioni non devono utilizzare URL basati su istanze.
- Accertarsi di aggiornare tutti gli URL delle applicazioni creati prima di avere abilitato un nome di dominio. Ad esempio, il campo `URL notifiche per email` in Risposte Chatter, se non viene aggiornato, continuerà a inviare notifiche con il vecchio URL agli utenti interni.
- se il dominio è stato registrato ma non è ancora stato distribuito, gli indirizzi URL visualizzeranno gli URL del dominio personale quando si esegue l'accesso dalla pagina di accesso Dominio personale. Tuttavia, i link che derivano da campi di unione incorporati nei messaggi email inviati in modo asincrono, ad esempio i messaggi del flusso di lavoro, conterranno ancora gli URL precedenti. Dopo aver distribuito il dominio, i link mostreranno i nuovi URL del dominio personale.
- Per aiutare gli utenti a iniziare a utilizzare il nuovo nome di dominio, fornire i link alle pagine che utilizzano spesso, come la pagina di accesso. Informare gli utenti se la policy di accesso verrà modificata e incoraggiarli ad aggiornare i segnalibri la prima volta che vengono reindirizzati.
- Utilizzare solo `Impedisci accesso da https://login.salesforce.com` per evitare che gli utenti che non conoscono il dominio personale possano tentare di utilizzarlo. In alternativa, mettere l'opzione a disposizione degli utenti quando acquisiscono dimestichezza con il nuovo nome di dominio.
- Scegliere l'opzione `Reindirizzamento con avviso alla stessa pagina all'interno del dominio` in `Policy di reindirizzamento` per dare il tempo agli utenti di aggiornare i propri segnalibri con il nuovo nome di dominio.

  Per introdurre gradualmente il nome di dominio agli utenti, è possibile utilizzare le impostazioni della policy di accesso del dominio. Il reindirizzamento degli utenti accompagnato da un avvertimento per alcuni giorni o alcune settimane prima di chiedere loro di utilizzare il nuovo nome di dominio per accedere alle pagine, darà agli utenti il tempo necessario a modificare i segnalibri.
- Se si decide di bloccare le richieste di pagine che non utilizzano gli URL del nuovo nome di dominio Salesforce, informare gli utenti che devono aggiornare i segnalibri o crearne di nuovi per la pagina di accesso e le schede e i link all'interno dell'applicazione. Se si cambiano i criteri di reindirizzamento all'accesso in `Nessun reindirizzamento`, agli utenti verrà richiesto di utilizzare i nuovi URL immediatamente.
- Se si utilizza Dominio personale, è possibile identificare gli utenti che accedono con il nuovo URL di accesso, nonché il momento dell'accesso. Da Imposta, immettere *`Cronologia accessi`* nella casella `Ricerca veloce`, quindi selezionare **Cronologia accessi** e visualizzare le colonne Nome utente e URL di accesso.
- Comunicare la modifica imminente agli utenti prima di distribuirla.
- Nella pagina `login.salesforce.com` gli utenti possono fare clic sul link **Accedi a un dominio personalizzato** per fornire il nome del dominio personalizzato e accedere. In questo caso, devono conoscere il nome del dominio. Tuttavia, è necessario fornire agli utenti un link diretto alla pagina di accesso del dominio personalizzato.

| Se si dispone di quanto segue | Effettuare queste operazioni |
|---|---|
| Integrazioni API nell'organizzazione | Verificare se il client API fa riferimento direttamente all'endpoint del server. Il client API deve utilizzare il valore LoginResult.serverURL restituito dalla richiesta di accesso anziché un URL del server a livello di codice.<br><br>Al termine della distribuzione del dominio personalizzato, Salesforce restituisce l'URL del server contenente il dominio. Anche se le impostazioni della policy di reindirizzamento non hanno effetto sulle chiamate API (le vecchie chiamate agli URL di istanza devono continuare a funzionare), la procedura consigliata è utilizzare il valore restituito da Salesforce. |
| Modelli di email | Sostituire i riferimenti all'URL dell'istanza dell'organizzazione con il proprio dominio personalizzato. |
| Pagine Visualforce personalizzate o applicazioni Force.com personalizzate | Sostituire i riferimenti all'URL dell'istanza dell'organizzazione con il proprio dominio personalizzato. Vedere l'articolo How to find hard-coded references with the Force.com IDE. |
| Chatter | Indicare agli utenti di aggiornare eventuali segnalibri nella barra di navigazione sinistra del gruppi Chatter. |
| Zone per le Comunità (Idee/Risposte/Risposte Chatter) | Aggiornare manualmente l'`URL notifica email`.<br><br>Per aggiornare l'URL, cancellare l'URL esistente in modo che il campo rimanga vuoto. Salvare la pagina: il sistema compila il campo con il nuovo URL del dominio personale. |

VEDERE ANCHE:

Modifiche dell'URL del Dominio personale

Verifica e distribuzione del nuovo nome di dominio

Panoramica su Dominio personale

## Verifica e distribuzione del nuovo nome di dominio

Dopo avere impostato il nome di dominio, verificarlo e distribuirlo agli utenti.

Prima di distribuire il dominio agli utenti, è possibile effettuare l'accesso per verificare il dominio. La verifica consente di esaminare il nome di dominio e di controllare gli indirizzi di pagine importanti che gli utenti dovranno utilizzare dopo che il dominio sarà stato distribuito.

Importante: Una volta distribuito il nuovo nome di dominio, non sarà più possibile annullarne la distribuzione.

1. Verificare l'accesso al dominio. Da Imposta, digitare *Dominio personale* nella casella Ricerca veloce, quindi selezionare **Dominio personale** e fare clic su **Fare clic qui per effettuare l'accesso**. Oppure, fare clic sull'URL contenuto nel messaggio per accedere a Salesforce utilizzando il nuovo nome di dominio.

   Prima di distribuire il dominio agli utenti, è possibile personalizzare la sua pagina di accesso e aggiungere i servizi di autenticazione (ad esempio l'accesso mediante social network). Inoltre, è possibile verificare i domini anche negli ambienti Sandbox. Tuttavia, prima di distribuire il dominio, non è possibile impostare una policy di accesso, ad esempio per impedire agli utenti di accedere da login.salesforce.com.

2. Effettuare il test sul nuovo nome di dominio facendo clic sulle schede e sui link all'interno dell'applicazione. Si noti che tutte le pagine mostrano il nuovo nome di dominio.

   Se si è deciso di personalizzare l'interfaccia utente di Salesforce con funzionalità quali pulsanti personalizzati o pagine Visualforce, effettuare una verifica degli elementi personalizzati prima di distribuire il nome di dominio. Le personalizzazioni non devono utilizzare URL basati su istanze.

3. Per distribuire il nuovo nome di dominio nell'organizzazione, da Imposta, immettere *Dominio personale* nella casella Ricerca veloce, quindi selezionare **Dominio personale** e fare clic su **Distribuisci agli utenti**.

Quando viene distribuito, il dominio viene attivato immediatamente e tutti gli utenti vengono reindirizzati alle pagine con i nuovi indirizzi del dominio. A questo punto, è possibile impostare le policy di accesso, nella sezione Impostazioni dominio che viene visualizzata dopo che è stato distribuito il dominio.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Performance Edition**, **Unlimited Edition**, **Enterprise Edition**, **Developer Edition**, **Professional Edition** e **Group Edition**.

AUTORIZZAZIONI UTENTE

Per impostare un nome di dominio:
- "Personalizza applicazione"

VEDERE ANCHE:

Impostazione di un nome di dominio

Linee guida e procedure consigliate per l'implementazione del dominio personale

Personalizzazione dell'immagine aziendale della pagina di accesso

Aggiunta di provider di identità a una pagina di accesso

Impostazione della policy di accesso del dominio personale

## Modifiche dell'URL del Dominio personale

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Performance Edition**, **Unlimited Edition**, **Enterprise Edition**, **Developer Edition**, **Professional Edition** e **Group Edition**.

Quando si imposta un nome di dominio per la propria organizzazione, tutti gli URL delle applicazioni, inclusi quelli delle pagine Visualforce, cambiano. Accertarsi di aggiornare tutti gli URL delle applicazioni creati prima di avere abilitato un nome di dominio. Ad esempio, il campo `URL notifiche per email` in Risposte Chatter, se non viene aggiornato, continuerà a inviare notifiche con il vecchio URL agli utenti interni. La seguente tabella mostra le differenze.

| Tipo di URL | URL precedente | Nuovo URL |
|---|---|---|
| Accesso | `https://login.salesforce.com` | `https://<subdomain>.my.salesforce.com` |
| Pagina o scheda dell'applicazione | `https://na1.salesforce.com/<pageID>` | `https://<subdomain>.my.salesforce.com/<pageID>` |
| Pagina Visualforce senza spazio dei nomi | `https://c.na1.visual.force.com/apex/<pagename>` | `https://<subdomain>--c.na1.visual.force.com/apex/<pagename>` |
| Pagina Visualforce *con* spazio dei nomi | `https://<yournamespace101>.na1.visual.force.com/apex/<pagename>` | `https://<subdomain>--<yournamespace>.na1.visual.force.com/apex/<pagename>` |

**Nota:** se si implementa Dominio personale in un ambiente Sandbox, il formato dell'URL è`https://<subdomain>--<sandboxname>.<instance>.my.salesforce.com`. Poiché non è possibile avere spazi dei nomi in un ambiente Sandbox, il formato di tutti gli URL delle pagine Visualforce in un Sandbox è `https://<subdomain>--<sandboxname>.<instance>.my.salesforce.com/apex/<pagename>`.

VEDERE ANCHE:

Panoramica su Dominio personale

Linee guida e procedure consigliate per l'implementazione del dominio personale

# Impostazione della policy di accesso del dominio personale

Proteggere l'accesso personalizzando la policy di accesso del proprio dominio.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Performance Edition**, **Unlimited Edition**, **Enterprise Edition**, **Developer Edition**, **Professional Edition** e **Group Edition**.

AUTORIZZAZIONI UTENTE

Per impostare la policy di accesso per un dominio:
- "Personalizza applicazione"

Personalizzare la policy di accesso per aggiungere un ulteriore livello di protezione dell'organizzazione. Per impostazione predefinita, gli utenti possono effettuare l'accesso da una pagina di accesso Salesforce generica, aggirando la pagina di accesso specifica del proprio dominio. Agli utenti è anche consentito effettuare richieste di pagine senza il nome del dominio, ad esempio utilizzando i vecchi segnalibri.

1. Da Imposta, digitare *`Dominio personale`* nella casella `Ricerca veloce` e quindi selezionare **Dominio personale**.
2. Da Impostazioni dominio personale, fare clic su **Modifica**.
3. Per disattivare l'autenticazione per gli utenti che non utilizzano la pagina di accesso specifica del dominio, selezionare la policy di accesso. In questo modo, ad esempio, si impedirà agli utenti di effettuare l'accesso dalla pagina di accesso generica `https://<istanza>.salesforce.com/` e di essere reindirizzati alle pagine dopo l'accesso. Questa opzione rafforza la protezione, impedendo tentativi di accesso da parte di chi non conosce il nome del dominio.
4. Scegliere i criteri di reindirizzamento.
   a. Scegliere `Reindirizzamento alla stessa pagina all'interno del dominio` per consentire agli utenti di continuare a utilizzare URL che non contengono il nome di dominio. La scelta di questa opzione non aumenta la protezione dell'organizzazione.
   b. Scegliere `Reindirizzamento con avviso alla stessa pagina all'interno del dominio` per avvertire gli utenti che dovrebbero utilizzare il nome del dominio. Dopo la lettura dell'avviso, agli utenti sarà consentito visualizzare la pagina. Scegliere questa opzione per alcuni giorni o alcune settimane aiuta gli utenti nella transizione al nuovo nome di dominio, ma non aumenta la protezione dell'organizzazione.
   c. Scegliere `Nessun reindirizzamento` per richiedere agli utenti di utilizzare il nome di dominio durante la visualizzazione delle pagine. Questa opzione offre il livello di protezione massimo.
5. Fare clic su **Salva**.

VEDERE ANCHE:

Impostazione di un nome di dominio

Linee guida e procedure consigliate per l'implementazione del dominio personale

## Personalizzazione dell'immagine aziendale della pagina di accesso

Personalizzare l'aspetto della pagina di accesso aggiungendo un colore di sfondo, il logo e il contenuto dell'iFrame destro. La personalizzazione della pagina di accesso consente agli utenti di riconoscerla collegandola all'immagine aziendale.

1. Da Imposta, digitare *`Dominio personale`* nella casella `Ricerca veloce` e quindi selezionare **Dominio personale**.
2. In Configurazione autenticazione, fare clic su **Modifica**.
3. Per personalizzare il logo, caricare un'immagine.

   Le immagini possono essere file .jpg, .gif o .png di dimensioni fino a 100 KB. Le dimensioni massime per l'immagine sono 250 pixel x 250 pixel.
4. Per personalizzare lo sfondo della pagina di accesso, fare clic sull'icona o immettere un codice colore esadecimale valido.
5. Immettere l'URL del file da includere nell'iFrame destro sulla pagina di accesso.

   Il file deve trovarsi in corrispondenza di un URL che utilizza la crittografia SSL e il prefisso https://. Le dimensioni massime del contenuto sono 478 pixel x 397 pixel.
6. Se lo si desidera, selezionare i servizi di autenticazione come provider di identità nella pagina di accesso, ad esempio provider di sign-on come Google o Facebook. Gli utenti possono quindi accedere con gli account di tali servizi. In Imposta, configurare i servizi di autenticazione come Provider di autenticazione.
7. Fare clic su **Salva**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Performance Edition**, **Unlimited Edition**, **Enterprise Edition**, **Developer Edition**, **Professional Edition** e **Group Edition**.

AUTORIZZAZIONI UTENTE

Per personalizzare una pagina di accesso:
- "Personalizza applicazione"

VEDERE ANCHE:

Impostazione di un nome di dominio

Aggiunta di provider di identità a una pagina di accesso

Impostazione della policy di accesso del dominio personale

Informazioni sui provider di autenticazione esterni

# Aggiunta di provider di identità a una pagina di accesso

Consentire agli utenti di eseguire l'autenticazione mediante opzioni alternative di provider di identità direttamente dalla propria pagina di accesso.

Se è stato abilitato Single Sign-On e si è configurato SAML, o se sono stati impostati provider di autenticazione esterni come Provider di autenticazione in Imposta, è possibile fornire i link a questi altri provider di identità nella pagina di accesso del proprio dominio. Gli utenti vengono indirizzati alla schermata di accesso del provider di identità alternativo per l'autenticazione e quindi reindirizzati a Salesforce.

Nota: I servizi di autenticazione disponibili includono tutti i provider configurati come provider di identità Single-Sign-On SAML o provider di autenticazione esterni, ad eccezione di Janrain. Janrain non può essere utilizzato per l'autenticazione dalla pagina di accesso.

1. Da Imposta, digitare `Dominio personale` nella casella `Ricerca veloce` e quindi selezionare **Dominio personale**.
2. In Configurazione autenticazione, fare clic su **Modifica**.
3. Selezionare uno o più servizi di autenticazione già configurati come provider di identità.
4. Fare clic su **Salva**.

VEDERE ANCHE:

Impostazione di un nome di dominio
Personalizzazione dell'immagine aziendale della pagina di accesso
Impostazione della policy di accesso del dominio personale
Informazioni sui provider di autenticazione esterni

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Performance Edition**, **Unlimited Edition**, **Enterprise Edition**, **Developer Edition**, **Professional Edition** e **Group Edition**.

AUTORIZZAZIONI UTENTE

Per aggiungere provider di identità a una pagina di accesso:

- "Personalizza applicazione"

## Ottenere informazioni sulle prestazioni e la manutenzione del sistema tramite Dominio personale

I clienti di Salesforce possono ottenere le informazioni relative alle prestazioni e alla manutenzione del sistema da `trust.salesforce.com`.

Di seguito è descritta la procedura per ottenere tali informazioni utilizzando il nuovo nome dominio.

1. Andare a trust.salesforce.com, dove è possibile verificare lo stato del sistema.
2. Per trovare l'istanza del proprio dominio, fare clic su **Quale istanza sto utilizzando?**
3. Nella tabella Stato del sistema, cercare la voce della propria istanza.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Performance Edition**, **Unlimited Edition**, **Enterprise Edition**, **Developer Edition**, **Professional Edition** e **Group Edition**.

AUTORIZZAZIONI UTENTE

Per impostare un nome di dominio:

- "Personalizza applicazione"

VEDERE ANCHE:

Panoramica su Dominio personale

## Domande frequenti sul dominio personale

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Performance Edition**, **Unlimited Edition**, **Enterprise Edition**, **Developer Edition** e **Database.com Edition**. Alcuni argomenti non sono validi per la versione **Database.com Edition**.

IN QUESTA SEZIONE:

È possibile rinominare o rimuovere il nome di dominio personalizzato?

## Che cos'è il Dominio personale?

Utilizzando il Dominio personale, gli amministratori possono definire un nome di dominio Salesforce personalizzato per la propria organizzazione. Il nome del dominio personalizzato appare in tutti gli URL dell'organizzazione e sostituisce il nome dell'istanza (ad esempio, `na1`). Per gli URL delle organizzazioni che utilizzano il Dominio personale viene utilizzato il formato `https://<miodominio>.my.salesforce.com` (ad esempio, `https://miodominio.my.salesforce.com`).

Il Dominio personale non viene utilizzato come dominio personalizzato per i siti, le comunità o i portali. I domini vengono definiti separatamente.

## In quali versioni di Salesforce è disponibile Dominio personale?

Performance Edition, Unlimited Edition, Enterprise Edition, Developer Edition, Professional Edition e Group Edition.

## Quali sono i vantaggi del dominio personale?

Il dominio personale consente ai clienti di:

- Personalizzare la pagina di accesso con la propria immagine aziendale.
- Utilizzare le funzioni di Identity per il Single Sign-On. Il dominio personale è richiesto per:
  - Single Sign-On a un'organizzazione Salesforce
  - Utilizzo di un'organizzazione Salesforce come provider di identità per il Single Sign-On ad applicazioni di terze parti o altre organizzazioni Salesforce
- Conservare i deep link (ad esempio `https://<mydomain>.my.salesforce.com/001/o`) in caso di ripartizioni e migrazioni future dell'organizzazione.

## Dominio personale funziona in modo diverso nelle varie versioni di Salesforce?

L'unica differenza consiste nel fatto che agli URL della versione Developer Edition viene aggiunto "-developer-edition".

## Il Dominio personale funziona nei Sandbox?

I Sandbox e le organizzazioni di produzione sono ambienti diversi e gestiscono registri separati dei nomi di dominio. Quindi, è possibile utilizzare lo stesso nome di Dominio personale nei Sandbox. Infatti, durante un aggiornamento del Sandbox, il nome del Dominio personale dell'organizzazione di produzione viene copiato nel Sandbox.

Ad esempio, se il nome dell'organizzazione di produzione è `acme.my.saleforce.com`, il nome del Sandbox è `acme--<nomeSandbox>.csN.my.salesforce.com`.

È necessario testare il dominio personalizzato in un Sandbox prima di distribuirlo per trovare eventuali riferimenti a livello di codice agli URL in pagine Visualforce, modelli di email o altri contenuti.

## Quali sono le differenze tra le opzioni di policy di reindirizzamento?

Dopo avere distribuito il dominio, è possibile selezionare un'opzione di reindirizzamento per consentire agli utenti di provare ad accedere a una pagina dell'organizzazione senza utilizzare il nome di dominio personalizzato.

Per visualizzare la policy assegnata, da Imposta, immettere *`Dominio personale`* nella casella `Ricerca veloce`, quindi selezionare **Dominio personale**.

Se l'opzione `Reindirizzamento alla stessa pagina all'interno del dominio` è selezionata, gli utenti vengono immediatamente indirizzati al nuovo URL, senza alcuna notifica.

Se è selezionata l'opzione `Reindirizzamento con avviso alla stessa pagina all'interno del dominio`, gli utenti visualizzano brevemente un messaggio di avviso prima di essere reindirizzati al nuovo URL. L'avviso offre agli utenti la possibilità di modificare i propri segnalibri e iniziare ad acquisire dimestichezza con il nuovo nome di dominio. Il messaggio non può essere personalizzato.

Se si seleziona l'opzione `Nessun reindirizzamento`, l'utente vede che la pagina è mancante. Questa è l'opzione consigliata poiché è la più sicura, ma può essere opportuno utilizzare `Reindirizzamento con avviso alla stessa pagina all'interno del dominio` per un breve periodo di tempo dopo la distribuzione del dominio, in modo tale che gli utenti si abituino ai nuovi URL.

## Come funziona il Dominio personale con il Single Sign-On?

Il Dominio personale è necessario per l'implementazione del Single Sign-On. Per le richieste di Single Sign-On in entrata, il dominio personalizzato abilita i deep link direttamente nelle pagine dell'organizzazione. Non sono richieste modifiche per il provider di identità. L'endpoint SAML di Salesforce (`login.salesforce.com`) continua a funzionare per le richieste SAML e OAUTH, anche se l'organizzazione distribuisce il Dominio personale e ha l'opzione `Impedisci accesso da https://login.salesforce.com` per gli utenti selezionata nelle impostazioni del Dominio personale.

Nota: se si utilizzano gruppi Chatter esterni insieme al Single Sign-On per i dipendenti, gli utenti all'esterno dell'azienda vengono reindirizzati a un provider di identità SAML a cui non possono accedere. Per fare in modo che l'implementazione funzioni, eseguire la migrazione dei gruppi Chatter esterni alle comunità oppure *non* selezionare `Impedisci accesso da https://login.salesforce.com` nelle impostazioni del Dominio personale. In questo modo gli utenti potranno continuare ad accedere tramite `login.salesforce.com`.

## Dominio personale è disponibile per l'API?

Sì, è possibile utilizzare le API Salesforce con il proprio Dominio personale.

## Il sottodominio di Dominio personale è correlato al sottodominio di Sites?

No. I sottodomini utilizzati per Sites e Dominio personale possono corrispondere o essere diversi.

## Esiste un limite alla lunghezza del sottodominio?

Sì. È possibile utilizzare fino a 40 caratteri. Il limite non si applica per il protocollo (`https://`) e il dominio (`my.salesforce.com`).

## Dopo aver impostato Dominio personale, sarà ancora possibile accedere da **`https://login.salesforce.com`**?

Sì, a meno che l'operazione non venga impedita dall'amministratore di sistema. In tal caso, sarà necessario eseguire l'accesso utilizzando il nuovo URL del Dominio personale.

## Sarà ancora possibile accedere da un URL contenente un'istanza di Salesforce, ad esempio **`https://na1.salesforce.com`**?

Sì, a meno che l'operazione non venga impedita dall'amministratore di sistema. In tal caso, sarà necessario eseguire l'accesso utilizzando il nuovo URL del Dominio personale.

### Sarà ancora possibile utilizzare i segnalibri precedenti di Salesforce?

Sì, se l'amministratore di sistema lo consente. In tal caso, gli utenti verranno reindirizzati alla pagina Salesforce utilizzando il nuovo URL di Dominio personale. Se l'amministratore di sistema non consente l'utilizzo dei vecchi segnalibri o viene visualizzato un avviso, sarà necessario aggiornare i segnalibri utilizzando il nuovo nome di dominio.

### Gli URL della pagina Visualforce e dei contenuti (file) verranno modificati?

Gli URL delle pagine Visualforce contengono il nuovo nome di dominio, ad esempio `https://<miodominio>--c.<istanza>.visual.force.com`.

Anche gli URL dei contenuti (file) contengono il nuovo nome di dominio, ad esempio `https://<miodominio>--c.<istanza>.content.force.com`.

### È possibile rinominare o rimuovere il nome di dominio personalizzato?

Non è possibile modificare il nome di dominio personalizzato, né invertirne la distribuzione, una volta distribuito. In caso sia assolutamente necessario modificarlo, contattare l'assistenza clienti di Salesforce.

# Programma di avvio app

## Abilitazione del programma di avvio app

Il programma di avvio app fornisce agli utenti dei loghi che consentono di accedere alle applicazioni locali, alle applicazioni connesse e alle app di Salesforce, tutto da un'interfaccia utente unificata. Gli amministratori possono impostare l'ordine predefinito delle app per le proprie organizzazioni.

Tutti gli utenti di Lightning Experience ricevono il programma di avvio app.

Gli utenti di Salesforce Classic devono disporre dell'autorizzazione "Utilizza funzioni Identity" e l'opzione Programma di avvio app impostata su **Visibile** nel proprio profilo. Gli utenti vedranno solo le app che sono autorizzati a vedere.

Gli amministratori di Salesforce Classic che utilizzano il profilo Amministratore di sistema hanno automaticamente accesso al programma di avvio app. Gli amministratori che utilizzano profili clonati dal profilo Amministratore di sistema non possono accedere automaticamente.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

IN QUESTA SEZIONE:

Abilitazione del programma di avvio app con un profilo in Salesforce Classic
È possibile creare un profilo e assegnarlo agli utenti in modo che possano accedere al programma di avvio app.

Abilitazione del programma di avvio app con un insieme di autorizzazioni in Salesforce Classic
È possibile creare un insieme di autorizzazioni e assegnarlo agli utenti in modo che possano accedere al programma di avvio app.

VEDERE ANCHE:

https://na1.salesforce.com/help/pdfs/en/salesforce_identity_implementation_guide.pdf

## Abilitazione del programma di avvio app con un profilo in Salesforce Classic

È possibile creare un profilo e assegnarlo agli utenti in modo che possano accedere al programma di avvio app.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Nota: queste operazioni funzionano in Salesforce Classic. Se nella parte alta della schermata compare una fila di schede, ci si trova in Salesforce Classic. Se a sinistra è presente una barra di navigazione, ci si trova in Lightning Experience.

Gli amministratori di Salesforce Classic che utilizzano il profilo Amministratore di sistema hanno automaticamente accesso al programma di avvio app. Gli amministratori che utilizzano profili clonati dal profilo Amministratore di sistema non possono accedere automaticamente.

1. Da Imposta, immettere *Profili* nella casella Ricerca veloce, quindi selezionare **Profili**.
2. Fare clic su **Nuovo profilo**.
3. Selezionare un profilo esistente come base per il nuovo profilo.
   Ad esempio, selezionare **Utente standard**.
4. Inserire il nome del nuovo profilo.
   Ad esempio, *Identità utente standard*.
5. Fare clic su **Salva**.
6. Nella pagina dei dettagli del nuovo profilo, fare clic su **Modifica**.
7. Nelle impostazioni delle app personalizzate, impostare il programma di avvio app su **Visibile**, se necessario.
   Nelle impostazioni delle schede, verificare che la scheda Programma di avvio app sia impostata su Impostazioni predefinite attivate.
8. In Autorizzazioni amministrative, selezionare **Utilizza funzioni Identity**.
9. Fare clic su **Salva**.
10. Da Imposta, immettere *Utenti* nella casella Ricerca veloce, quindi selezionare **Utenti**.
11. Fare clic su **Modifica** accanto a ciascun utente che dovrà accedere al programma di avvio app.
12. Nel campo Profilo dell'utente, selezionare il nuovo profilo con l'opzione "Utilizza funzioni Identity" abilitata.
    Ad esempio, si può utilizzare il profilo *Identità utente standard*.
13. Fare clic su **Salva**.
    Quando si accede come utente selezionato, il programma di avvio app appare nel menu a discesa delle app.

VEDERE ANCHE:

Abilitazione del programma di avvio app

## Abilitazione del programma di avvio app con un insieme di autorizzazioni in Salesforce Classic

È possibile creare un insieme di autorizzazioni e assegnarlo agli utenti in modo che possano accedere al programma di avvio app.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Nota: queste operazioni funzionano in Salesforce Classic. Se nella parte alta della schermata compare una fila di schede, ci si trova in Salesforce Classic. Se a sinistra è presente una barra di navigazione, ci si trova in Lightning Experience.

1. Da Imposta, immettere *Insiemi di autorizzazioni* nella casella `Ricerca veloce`, quindi selezionare **Insiemi di autorizzazioni**.
2. Fare clic su **Nuovo**.
3. Immettere un'etichetta per il nuovo insieme di autorizzazioni.

   Ad esempio, *Funzioni Identity*.
4. Se lo si desidera, limitare l'uso dell'insieme di autorizzazioni a una licenza utente specifica.
5. Fare clic su **Salva**.
6. Fare clic su **Autorizzazioni di sistema**.
7. Fare clic su **Modifica**.
8. Selezionare **Utilizza funzioni Identity**.
9. Fare clic su **Salva**.
10. Da Imposta, immettere *Utenti* nella casella `Ricerca veloce`, quindi selezionare **Utenti**.
11. Fare clic sul nome di un utente esistente a cui si desidera fornire l'accesso al programma di avvio app.
12. Nell'elenco correlato **Assegnazioni dell'insieme di autorizzazioni**, fare clic su **Modifica assegnazioni**.
13. Aggiungere il nuovo insieme di autorizzazioni creato per le funzioni di Identity agli insiemi di autorizzazioni abilitati.
14. Fare clic su **Salva**.

    Quando si accede come utente selezionato, il programma di avvio app appare nel menu a discesa delle app.

    Nota: Se il programma di avvio app ancora non appare: nel profilo associato all'utente, selezionare **Visibile** per l'impostazione del programma di avvio app.

VEDERE ANCHE:

Abilitazione del programma di avvio app

# Configurazione delle impostazioni di protezione per il caricamento e il download dei file

Per motivi di sicurezza, è possibile che l'organizzazione desideri configurare le modalità di gestione di alcuni tipi di file durante il caricamento e il download.

Per gestire le impostazioni di caricamento e download dei file:

1. Da Imposta, immettere *Sicurezza caricamento e download dei file* nella casella `Ricerca veloce`, quindi selezionare **Sicurezza caricamento e download dei file**.
2. Fare clic su **Modifica**.
3. Per impedire agli utenti di caricare file che potrebbero rappresentare un rischio per la sicurezza, selezionare `Non consentire il caricamento di file HTML come allegati o record di documenti`.

   Questa impostazione blocca il caricamento dei seguenti tipi di file MIME: `.html`, `.htt`, `.mht`, `.svg`, `.swf`, `.thtml` e `.xhtml`.

   Avvertenza: Quando si seleziona questa opzione, tenere presente quanto segue:

   - Se l'organizzazione utilizza il Portale partner per concedere ai partner l'accesso a Salesforce, si consiglia di non abilitare questa impostazione. L'abilitazione di questa impostazione impedisce all'organizzazione di personalizzare l'aspetto del proprio Portale partner.
   - gli allegati HTML non sono consentiti con le soluzioni, indipendentemente dall'abilitazione o meno di questa impostazione di sicurezza. Inoltre questa impostazione non si applica agli allegati dei modelli di email: gli allegati HTML nei modelli di email, infatti, sono sempre consentiti.
   - L'abilitazione di questa impostazione non incide sui documenti e gli allegati HTML caricati in precedenza. Tuttavia, quando gli utenti tentano di visualizzare un allegato HTML o un documento, il browser chiede di aprire tali allegati nel browser, salvarli sul computer oppure annullare l'azione.

4. Impostare il comportamento per il download di ogni tipo di file:
   a. **Scarica** (consigliato): il file viene sempre scaricato, di qualunque tipo esso sia.
   b. **Esegui nel browser**: il file, di qualunque tipo esso sia, viene visualizzato ed eseguito automaticamente quando aperto in un browser o tramite una richiesta HTTP.
   c. **Ibrido**: il file utilizza il comportamento di esecuzione predefinito del browser, ma scarica i file Chatter e Salesforce CRM Content.
5. Fare clic su **Salva**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

AUTORIZZAZIONI UTENTE

Per configurare le impostazioni di caricamento e download dei file:

- "Personalizza applicazione"

# Protezione delle connessioni

## Informazioni su Single Sign-On

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

L'autenticazione federata è disponibile in: **tutte** le versioni

L'autenticazione delegata è disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

I provider di autenticazione sono disponibili nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:
- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:
- "Personalizza applicazione"

  E

  "Modifica tutti i dati"

Single sign-on è un processo che consente agli utenti di rete di accedere a tutte le risorse di rete autorizzate senza dover eseguire un accesso separato per ciascuna risorsa. Single Sign-On consente di convalidare i nomi utente e le password confrontandoli con quelli presenti nel database aziendale degli utenti o in un'altra applicazione client anziché avere password utente separate gestite da Salesforce.

Salesforce consente di utilizzare Single Sign-On nei modi seguenti:

- L'autenticazione federata con SAML (Security Assertion Markup Language) consente di inviare i dati di autenticazione e autorizzazione tra servizi Web affiliati ma non correlati. In questo modo è possibile accedere a Salesforce da un'applicazione client. L'autenticazione federata con SAML è abilitata per impostazione predefinita per l'organizzazione.
- Il Single Sign-On con autenticazione delegata consente di integrare Salesforce con un metodo di autenticazione prescelto. Ciò permette di integrare l'autenticazione con il server LDAP (Lightweight Directory Access Protocol) o di eseguire l'accesso con Single sign-on effettuando l'autenticazione tramite un token anziché una password. L'autenticazione delegata viene gestita a livello di autorizzazione, consentendo ad alcuni utenti di utilizzare l'autenticazione delegata mentre altri continuano a utilizzare le loro password gestite da Salesforce. L'autenticazione delegata è impostata per autorizzazione e non a livello di organizzazione.

  I motivi principali per utilizzare l'autenticazione delegata comprendono:

  - Utilizzare un tipo di autenticazione utente più potente, quale l'integrazione con un provider d'identità sicuro
  - Rendere privata la pagina di accesso in modo che sia protetta dal firewall aziendale
  - Differenziare la propria organizzazione da tutte le altre società che utilizzano Salesforce per ridurre gli attacchi di phishing.

  È necessario richiedere che questa funzione sia abilitata da Salesforce. Per abilitare single sign-on mediante autenticazione delegata nella propria organizzazione, contattare Salesforce.
- I provider di autenticazione consentono agli utenti di accedere all'organizzazione Salesforce con le credenziali di accesso fornite da un provider di servizi esterno. Salesforce supporta il protocollo OpenId Connect che permette agli utenti di accedere da qualsiasi provider OpenID come Google, Paypal, LinkedIn e altri servizi che supportano OpenID Connect. Quando i provider di autenticazione sono abilitati, Salesforce non convalida la password dell'utente. Per definire le credenziali di autenticazione, Salesforce utilizza invece le credenziali di accesso dell'utente fornite da un provider di servizi esterno.

Quando si dispone di un provider di identità esterno e si configura single sign-on per l'organizzazione Salesforce, Salesforce funge da *fornitore di servizi.*. Inoltre, è possibile abilitare Salesforce come provider di identità e utilizzare single sign-on per collegarsi a un fornitore di servizi diverso. Solo il fornitore di servizi deve configurare single sign-on.

La pagina delle impostazioni Single Sign-On visualizza la versione di single sign-on disponibile per l'organizzazione. Per ulteriori informazioni sulle impostazioni single sign-on, vedere Configurazione delle impostazioni di SAML per Single Sign-On. Per ulteriori informazioni su SAML e la protezione Salesforce, vedere la *Guida all'implementazione delle misure di sicurezza*.

## Vantaggi di Single Sign-On

L'implementazione di single sign-on nell'organizzazione può offrire i seguenti vantaggi:

- **Riduzione dei costi amministrativi:** grazie a single sign-on, gli utenti devono memorizzare una sola password per accedere sia alle risorse di rete o applicazioni esterne sia a Salesforce. L'accesso degli utenti a Salesforce dall'interno della rete aziendale avviene in modo semplice e senza interruzioni e non viene richiesta l'immissione di nomi utente o password. Quando accedono a Salesforce dall'esterno della rete aziendale, gli utenti possono utilizzare la procedura di accesso alla rete aziendale. Dovendo gestire meno password, gli amministratori del sistema ricevono un numero inferiore di richieste di reimpostazione delle password dimenticate.
- **Sfruttamento degli investimenti esistenti:** molte aziende utilizzano un database LDAP centrale per gestire le identità degli utenti. La delega dell'autenticazione Salesforce a questo sistema fa sì che un utente rimosso dal sistema LDAP non possa più accedere a Salesforce; di conseguenza, gli utenti che lasciano l'azienda perdono automaticamente l'accesso ai dati aziendali.
- **Risparmio di tempo:** un utente impiega in media da 5 a 20 secondi per accedere a un'applicazione online, di più se commette un errore di digitazione del nome utente o della password e deve ripetere l'operazione. Grazie a single sign-on non è più necessario accedere manualmente a Salesforce e tutti i secondi risparmiati in questo modo contribuiscono a un incremento della produttività.
- **Maggior adozione da parte degli utenti:** poiché non devono eseguire alcuna procedura di accesso, è più probabile che gli utenti utilizzino Salesforce regolarmente. Ad esempio, gli utenti possono inviare messaggi di posta elettronica contenenti link a informazioni presenti in Salesforce quali record e rapporti e, quando il destinatario del messaggio seleziona tali link, la corrispondente pagina di Salesforce si apre automaticamente.
- **Maggior protezione:** la politica delle password in vigore per la rete aziendale verrà applicata anche a Salesforce. Inoltre, l'invio di una credenziale di autenticazione valida per un unico utilizzo può incrementare la sicurezza per gli utenti che hanno accesso a dati sensibili.

IN QUESTA SEZIONE:

Procedure consigliate per l'implementazione di Single Sign-On

Descrizione di Single Sign-On mediante autenticazione delegata

Configurazione di Salesforce per l'autenticazione delegata

Controllo dell'accesso dei singoli client API all'organizzazione Salesforce

Con il whitelisting dei client API è possibile imporre restrizioni a tutte le applicazioni client API, ad esempio Data Loader, in modo che richiedano l'approvazione dell'amministratore a meno che il profilo o l'insieme di autorizzazioni dell'utente sia dotato dell'autorizzazione "Utilizza qualsiasi client API".

Visualizzazione di errori di accesso Single Sign-On

## Procedure consigliate per l'implementazione di Single Sign-On

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

L'autenticazione federata è disponibile in: **tutte** le versioni

L'autenticazione delegata è disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

I Portali Clienti e i portali partner non sono disponibili nella versione **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:

- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:

- "Personalizza applicazione"

  E

  "Modifica tutti i dati"

Salesforce consente di utilizzare Single Sign-On nei modi seguenti:

- L'autenticazione federata con SAML (Security Assertion Markup Language) consente di inviare i dati di autenticazione e autorizzazione tra servizi Web affiliati ma non correlati. In questo modo è possibile accedere a Salesforce da un'applicazione client. L'autenticazione federata con SAML è abilitata per impostazione predefinita per l'organizzazione.
- Il Single Sign-On con autenticazione delegata consente di integrare Salesforce con un metodo di autenticazione prescelto. Ciò permette di integrare l'autenticazione con il server LDAP (Lightweight Directory Access Protocol) o di eseguire l'accesso con Single sign-on effettuando l'autenticazione tramite un token anziché una password. L'autenticazione delegata viene gestita a livello di autorizzazione, consentendo ad alcuni utenti di utilizzare l'autenticazione delegata mentre altri continuano a utilizzare le loro password gestite da Salesforce. L'autenticazione delegata è impostata per autorizzazione e non a livello di organizzazione.

  I motivi principali per utilizzare l'autenticazione delegata comprendono:

  - Utilizzare un tipo di autenticazione utente più potente, quale l'integrazione con un provider d'identità sicuro
  - Rendere privata la pagina di accesso in modo che sia protetta dal firewall aziendale
  - Differenziare la propria organizzazione da tutte le altre società che utilizzano Salesforce per ridurre gli attacchi di phishing.

  È necessario richiedere che questa funzione sia abilitata da Salesforce. Per abilitare single sign-on mediante autenticazione delegata nella propria organizzazione, contattare Salesforce.
- I provider di autenticazione consentono agli utenti di accedere all'organizzazione Salesforce con le credenziali di accesso fornite da un provider di servizi esterno. Salesforce supporta il protocollo OpenId Connect che permette agli utenti di accedere da qualsiasi provider OpenID come Google, Paypal, LinkedIn e altri servizi che supportano OpenID Connect. Quando i provider di autenticazione sono abilitati, Salesforce non convalida la password dell'utente. Per definire le credenziali di autenticazione, Salesforce utilizza invece le credenziali di accesso dell'utente fornite da un provider di servizi esterno.

È anche possibile configurare SAML per l'uso con i portali e per i Siti.

### Procedure consigliate per l'autenticazione delegata

Durante l'implementazione di single sign-on mediante autenticazione delegata per l'organizzazione, tenere presente le seguenti procedure consigliate.

- L'implementazione del servizio Web dell'organizzazione deve essere accessibile da parte dei server di Salesforce. Questo significa che è necessario distribuire il servizio Web su un server in DMZ. Ricordare di utilizzare il nome DNS esterno del server quando si immette l'`URL gateway delegato` nella sezione Autenticazione delegata di Salesforce (da Imposta, immettere *`Impostazioni Single Sign-On`* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni Single Sign-On**).
- Se Salesforce e il proprio sistema non si collegano o se l'elaborazione della richiesta dura più di 10 secondi, il tentativo di accesso non riesce. All'utente viene notificato un errore in cui si indica che il servizio di autenticazione aziendale non è al momento disponibile.
- Gli spazi dei nomi, i nomi di elementi e le lettere maiuscole/minuscole devono essere esatti nelle richieste SOAP. Quando possibile, per garantire l'accuratezza, si consiglia di generare lo stub del server da WSDL.
- Per motivi di sicurezza, è opportuno rendere disponibile il servizio Web tramite TLS. Utilizzare un certificato proveniente da un provider attendibile quale Verisign o Thawte. Per un elenco completo dei provider attendibili, contattare Salesforce.

- L'indirizzo IP che ha dato origine alla richiesta di accesso è `sourceIp`. Utilizzare questa informazione per limitare l'accesso in base alla posizione dell'utente. Tenere presente che la funzione Salesforce che esegue la convalida degli intervalli IP di accesso rimane in vigore per gli utenti Single Sign-On. Per ulteriori informazioni, vedere Impostazione delle restrizioni di accesso a pagina 515.
- Potrebbe essere necessario eseguire la mappatura tra i nomi utente interni dell'organizzazione e i nomi utente di Salesforce. Se l'organizzazione non segue una mappatura standard, potrebbe essere possibile estendere lo schema del database utenti (ad esempio, Elenco attivo) in modo da includere il nome utente Salesforce sotto forma di attributo di un account utente. Il servizio di autenticazione può quindi utilizzare questo attributo per eseguire la mappatura a un account utente.
- Si consiglia di non abilitare Single Sign-On per gli amministratori di sistema. Se gli amministratori di sistema sono utenti single sign-on e il server single sign-on ha un guasto, non potranno accedere a Salesforce. Gli amministratori di sistema dovrebbero sempre potere accedere a Salesforce in modo da potere disabilitare il servizio di single sign-on in caso di problema.
- Prima di implementare nella propria organizzazione una soluzione Single sign-on che si sta sviluppando, si consiglia di utilizzare un account Developer Edition o un Sandbox. Per registrarsi per un account gratuito della versione Developer Edition, andare a developer.salesforce.com.
- Accertarsi di eseguire un test dell'implementazione con i client Salesforce come Salesforce per Outlook, Connect per Office e Connect Offline. Per ulteriori informazioni, vedere Single Sign-On for Salesforce clients.

## Procedure consigliate per l'autenticazione federata mediante SAML

Durante l'implementazione di single sign-on federato mediante SAML per l'organizzazione, tenere presente le seguenti procedure consigliate.

- Annotare il valore `URL di accesso Salesforce` presente nella pagina di configurazione Impostazioni Single Sign-On e inserirlo nel parametro di configurazione corrispondente del provider di identità (noto a volte come "URL destinatario").
- Salesforce ammette un massimo di 3 minuti di differenza con l'orologio del server IDP; accertarsi che l'orologio del server sia aggiornato.
- Se non si è in grado di accedere con l'asserzione SAML, controllare sempre la cronologia degli accessi e annotare il messaggio di errore. Per risolvere i problemi, utilizzare il Validatore asserzione SAML nella pagina di configurazione Impostazioni Single Sign-On.
- È necessario mappare i nomi utente interni dell'organizzazione e i nomi utente Salesforce. Per fare questo è possibile procedere in due modi: aggiungere un ID univoco al campo `FederationIdentifier` di ciascun utente Salesforce, oppure estendere il proprio schema di database utente (ad esempio, Active Directory) per includere il nome utente Salesforce come un attributo di un account utente. Scegliere l'opzione corrispondente per il campo `Tipo ID utente SAML` e configurare il proprio servizio di autenticazione in modo che invii l'ID nelle asserzioni SAML.
- Prima di consentire agli utenti di accedere con le asserzioni SAML, abilitare la preferenza SAML dell'organizzazione e fornire tutte le configurazioni necessarie.
- Utilizzare la funzione Dominio personale per impedire agli utenti di accedere direttamente a Salesforce e garantire agli amministratori un maggiore controllo sui criteri di accesso. Si possono utilizzare i parametri URL forniti nel valore `URL di accesso Salesforce` della pagina di configurazione Impostazioni Single Sign-On con il proprio dominio personalizzato.

  Ad esempio, se l'`URL di accesso Salesforce` è `https://login.salesforce.com/?saml=02HKiP...`

  è possibile utilizzare `https://<my_domain_name>.my.salesforce.com/?saml=02HKiP...`
- Per il test di una soluzione Single sign-on SAML, si consiglia di utilizzare un account Developer Edition o un Sandbox. Per registrarsi per un account gratuito della versione Developer Edition, andare a developer.salesforce.com.
- Le copie del Sandbox sono eseguite con l'autenticazione federata con SAML disabilitato. Vengono conservate tutte le informazioni di configurazione, tranne il valore di `URL di accesso Salesforce`. L'`URL di accesso Salesforce` viene aggiornato in modo che corrisponda all'URL Sandbox, per esempio `http://cs1.salesforce.com`, dopo che SAML è stato nuovamente abilitato. Per abilitare SAML nel Sandbox, da Imposta immettere *`Impostazioni Single Sign-On`* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni Single Sign-On**, fare clic su **Modifica** e selezionare `SAML abilitato`.

- Il provider di identità deve consentire l'impostazione dell'URL pubblico del provider di servizi Il valore deve corrispondere al valore `ID entità` nella configurazione single sign-on. Il valore predefinito è `https://saml.salesforce.com`.

## Procedure consigliate di Single Sign-On per i portali

A partire dal rilascio Summer '13, i Portali Clienti e i Portali partner non sono disponibili per le nuove organizzazioni. Utilizzare invece le comunità. Per ulteriori informazioni sul Single Sign-On e su SAML per le comunità, vedere "Configurazione di SAML per le comunità" in Suggerimenti introduttivi sulle comunità. Se si continua a utilizzare i portali, tenere presente quanto segue.

- Solo SAML versione 2.0 può essere utilizzato con i portali.
- Sono supportati solo i Portali Clienti e i Portali partner.
- L'accesso avviato dal provider di servizi non è supportato.
- Per Single Sign-On per i portali sono richiesti entrambi gli attributi `portal_id` e `organization_id`. Se viene specificato un solo attributo, l'utente riceve un messaggio di errore.
- Se vengono specificati entrambi gli attributi `portal_id` e `organization_id` nell'asserzione SAML, l'utente viene indirizzato all'accesso al portale. Se non viene specificato nessuno dei due attributi, l'utente viene indirizzato al normale accesso Salesforce SAML.
- È possibile utilizzare più di un portale con un sola organizzazione.

## Procedure consigliate di Single Sign-On per i Siti

- Solo SAML versione 2.0 può essere utilizzato con i Siti.
- Sono supportati solo i Portali Clienti e i Portali partner.
- L'accesso avviato dal provider di servizi non è supportato.
- Per il Single Sign-On per i Siti sono richiesti gli attributi `portal_id`, `organization_id` e `siteUrl`. Se viene specificato un solo attributo, l'utente riceve un messaggio di errore.
- Se nell'asserzione SAML vengono specificati tutti e tre gli attributi `portal_id`, `organization_id` e `siteUrl`, l'utente viene indirizzato all'accesso ai Siti. Se `siteUrl` non è popolato e gli altri due attributi lo sono, l'utente viene indirizzato all'accesso a quel portale.
- È possibile utilizzare più di un portale con un sola organizzazione.

VEDERE ANCHE:

Informazioni su Single Sign-On

## Descrizione di Single Sign-On mediante autenticazione delegata

Salesforce utilizza la seguente procedura per autenticare gli utenti mediante Single Sign-On con autenticazione delegata:

1. Quando un utente cerca di accedere online oppure mediante API, Salesforce convalida il nome utente e controlla le autorizzazioni e le impostazioni di accesso dell'utente.
2. Se l'utente dispone dell'autorizzazione "È abilitato per Single Sign-On", Salesforce non convalida il nome utente e la password. Al contrario, viene eseguita una chiamata ai servizi Web dell'organizzazione dell'utente, con la richiesta di convalidare il nome utente e la password.

   Nota: Salesforce non archivia, registra o visualizza in alcun modo la password. che viene eliminata immediatamente al termine del processo.

3. La chiamata ai servizi Web trasmette `nome utente`, `password` e `sourceIp` al servizio Web. (`sourceIp` è l'indirizzo IP che ha dato origine alla richiesta di accesso. È necessario creare e distribuire un'implementazione del servizio Web a cui i server Salesforce possano accedere.)
4. L'implementazione del servizio Web convalida le informazioni trasmesse e restituisce `true` o `false`.
5. Se la risposta è `true`, la procedura di accesso continua, viene generata una nuova sessione e l'utente accede all'applicazione; al contrario, se viene restituito `false`, l'utente viene informato del fatto che la combinazione nome utente/password non è risultata valida.

Nota: Prima che un utente possa eseguire l'accesso dopo l'assegnazione dell'autenticazione delegata può verificarsi un momentaneo ritardo dovuto al tempo necessario per rendere disponibile l'account del nuovo utente nell'organizzazione.

VEDERE ANCHE:

Informazioni su Single Sign-On

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:

- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:

- "Personalizza applicazione"

  E

  "Modifica tutti i dati"

## Configurazione di Salesforce per l'autenticazione delegata

Per abilitare single sign-on (SSO) mediante autenticazione delegata nella propria organizzazione:

1. Per abilitare single sign-on mediante autenticazione delegata nella propria organizzazione, contattare Salesforce.
2. Creare il proprio servizio Web single sign-on:
   a. In Salesforce, scaricare il file WSDL (Web Services Description Language) `AuthenticationService.wsdl` da Imposta immettendo *Scarica WSDL autenticazione delegata* nella casella `Ricerca veloce` e quindi selezionando **Scarica WSDL autenticazione delegata**. Il file WSDL descrive il servizio di Single Sign-On per l'autenticazione delegata e può essere utilizzato per generare automaticamente uno stub lato server a cui è possibile aggiungere la propria implementazione specifica. Ad esempio, nello strumento WSDL2Java di Apache Axis, è possibile utilizzare lo switch `--server-side`. Nello strumento wsdl.exe di .NET, è possibile utilizzare lo switch `/server`.

      Per un esempio di richiesta e risposta, vedere Esempio di messaggio SOAP per l'autenticazione delegata a pagina 576.

   b. Aggiungere un link all'intranet aziendale o a un altro sito accessibile internamente che prende le credenziali utente autenticate e le trasmette mediante HTTP POST alla pagina di accesso di Salesforce.

      Poiché Salesforce utilizza il campo `password` solo per ritrasmetterlo nuovamente all'utente, non è necessario inviare una password in questo campo. Al contrario, è possibile trasmettere un altro token di autenticazione, quale un ticket Kerberos in modo che le password aziendali non vengano trasmesse a o da Salesforce.

      È possibile configurare l'autorità di autenticazione delegata Salesforce in modo che vengano consentiti solo i token oppure che vengano accettati sia token sia password. Se l'autorità accetta solo i token, un utente Salesforce non potrà accedere direttamente a Salesforce in quanto non può creare un token valido. Tuttavia, molte aziende scelgono di consentire sia i token sia le password. In questo ambiente, un utente potrà ancora accedere a Salesforce mediante la pagina di accesso.

      Quando il server Salesforce ritrasmette queste credenziali all'utente nel messaggio `Authenticate`, verificare le credenziali e accedere all'applicazione.

3. In Salesforce, specificare l'URL del gateway Single Sign-On dell'organizzazione: da Imposta, immettere *Single Sign-On* nella casella `Ricerca veloce`, selezionare **Impostazioni Single Sign-On** e fare clic su **Modifica**. Immettere l'URL nella casella di testo **URL gateway delegato**.

   Per motivi di sicurezza, Salesforce limita le porte in uscita che si possono specificare a uno dei seguenti valori:

   - 80: questa porta accetta solo connessioni HTTP.
   - 443: questa porta accetta solo connessioni HTTPS.
   - 1024-66535 (comprese): queste porte accettano connessioni HTTP o HTTPS.

4. In via facoltativa, selezionare la casella **Forza chiamata autenticazione delegata**.

   Nota: quando questa casella è deselezionata, all'endpoint SSO non viene effettuata una chiamata se il primo tentativo di accesso non riesce a causa di restrizioni presenti all'interno dell'organizzazione Salesforce. Se si necessita di registrare ogni tentativo di accesso, selezionare questa casella in modo da forzare una chiamata all'endpoint SSO a prescindere dagli errori causati da restrizioni di accesso.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:
- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:
- "Personalizza applicazione"

  E

  "Modifica tutti i dati"

5. Abilitare l'autorizzazione "È abilitato per Single Sign-On".

**Importante:** Per informazioni su come visualizzare gli errori di accesso, vedere Visualizzazione di errori di accesso Single Sign-On a pagina 556.

VEDERE ANCHE:

Informazioni su Single Sign-On

Descrizione di Single Sign-On mediante autenticazione delegata

## Controllo dell'accesso dei singoli client API all'organizzazione Salesforce

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:
- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:
- "Personalizza applicazione"

  E

  "Modifica tutti i dati"

Con il whitelisting dei client API è possibile imporre restrizioni a tutte le applicazioni client API, ad esempio Data Loader, in modo che richiedano l'approvazione dell'amministratore a meno che il profilo o l'insieme di autorizzazioni dell'utente sia dotato dell'autorizzazione "Utilizza qualsiasi client API".

Gli amministratori possono concedere l'accesso API ad alcuni utenti tramite l'autorizzazione "API abilitata". Una volta assegnata, questa autorizzazione consente all'utente l'accesso API tramite qualsiasi client (ad esempio Data Loader, Salesforce1, Salesforce per Outlook o lo strumento di migrazione Force.com). Per un controllo più puntuale sulle applicazioni utilizzabili dall'utente per l'accesso API è possibile implementare il whitelisting dei client API. Questa funzione sfrutta le capacità di autorizzazione esistenti delle applicazioni connesse. Con il whitelisting dei client API, un amministratore può approvare o bloccare l'accesso delle singole applicazioni client per ogni applicazione connessa associata. A tutte le applicazioni client non configurate come applicazioni connesse viene impedito l'accesso. Se non si utilizzano le applicazioni connesse è possibile allentare questa restrizione per i singoli utenti assegnando loro un profilo o un insieme di autorizzazioni in cui sia abilitata l'autorizzazione "Utilizza qualsiasi client API".

**Nota:** per abilitare il whitelisting dei client API, rivolgersi a Salesforce. Dopo l'abilitazione, tutti gli accessi client sono limitati se non sono esplicitamente consentiti dall'amministratore. Questa restrizione potrebbe bloccare l'accesso ad applicazioni che gli utenti utilizzano già. Prima di abilitare questa funzione è necessario configurare e approvare applicazioni connesse per tutte le applicazioni client che gli utenti devono poter continuare a utilizzare, o assegnare agli utenti un profilo o un insieme di autorizzazioni in cui sia abilitato "Utilizza qualsiasi client API".

Per configurare il whitelisting dei client API, procedere nel modo seguente.

1. Contattare Salesforce per far attivare la funzionalità per l'organizzazione.
2. Da Imposta, immettere *`Applicazioni connesse`* nella casella `Ricerca veloce`, quindi selezionare l'opzione di gestione delle applicazioni connesse.
3. In Impostazioni di accesso alle applicazioni, fare clic su **Modifica**.
4. Selezionare **Limitare l'accesso API alle applicazioni connesse installate con la policy "Gli utenti approvati dall'amministratore sono pre-autorizzati"**.

   Se lo si desidera, selezionare **Consenti alle pagine Visualforce di ignorare questa restrizione** in modo che le pagine Visualforce che utilizzano l'API continuino a essere autorizzate ad accedere agli oggetti nell'organizzazione. Se si abilita il whitelisting dei client API senza selezionare questa opzione, solo le applicazioni connesse approvate sono autorizzate e le pagine Visualforce potrebbero comportarsi in modo imprevisto. Inoltre, se l'opzione non è selezionata, alle applicazioni client che chiamano `getSessionId()` viene negato l'accesso. Le applicazioni che effettuano chiamate API a Salesforce utilizzando una sessione ottenuta in un contesto Visualforce non sono autorizzate ad accedere a meno che non si selezioni questa casella di controllo.

5. Fare clic su **Salva**.

Quando questa funzione è selezionata, tutte le applicazioni client necessitano dell'approvazione esplicita di un amministratore per essere autorizzate per l'organizzazione, a meno che l'utente non abbia un profilo o un insieme di autorizzazioni con "Utilizza qualsiasi client API" abilitato.

Alcuni componenti di applicazioni di uso comune vengono installati automaticamente come applicazioni connesse nelle organizzazioni. Questi componenti supportano applicazioni come Data Loader, Salesforce1, Workbench e simili. Quando si seleziona questa funzione, anche questi componenti richiederanno l'approvazione a meno che l'utente non abbia un profilo o un insieme di autorizzazioni con "Utilizza qualsiasi client API" abilitato. Per ulteriori informazioni su questi componenti, vedere Gestione di un'applicazione connessa.

## Visualizzazione di errori di accesso Single Sign-On

Se l'organizzazione è abilitata per Single Sign-On mediante autenticazione delegata e ha creato una soluzione Single Sign-On, è possibile visualizzare gli errori di accesso Single Sign-On più recenti dell'organizzazione.

1. Da Imposta, immettere *`Cronologia errori autenticazione delegata`* nella casella `Ricerca veloce`, quindi selezionare **Cronologia errori autenticazione delegata**.
2. Per i venti errori di accesso Single Sign-On più recenti, è possibile visualizzare il nome utente, l'ora di accesso e l'errore.

AUTORIZZAZIONI UTENTE

Per visualizzare gli errori di accesso Single Sign-On:

- "Modifica tutti i dati"

Nota: per ulteriori informazioni sull'abilitazione Single Sign-On per l'organizzazione, rivolgersi a Salesforce.

VEDERE ANCHE:

Informazioni su Single Sign-On

# Informazioni su SAML

SAML (Security Assertion Markup Language) è uno standard basato su XML che consente di trasmettere le decisioni relative all'autenticazione da un servizio a un altro e sta alla base di molte soluzioni di single sign-on per il Web. Salesforce supporta SAML per il Single Sign-On in Salesforce da un portale aziendale o un provider di identità.

Molte delle operazioni necessarie all'impostazione di Single Sign-On mediante SAML avvengono con il provider di identità:

1. Definire un provider di identità SAML e raccogliere le informazioni sulle modalità di connessione a Salesforce. Si tratta del provider che invierà le richieste Single sign-on a Salesforce.
2. Fornire le informazioni al provider di identità, ad esempio gli URL delle pagine di avvio, accesso e disconnessione.
3. Configurare Salesforce utilizzando le istruzioni contenute in Configurazione delle impostazioni di SAML per Single Sign-On. Questa è l'unica operazione che viene eseguita in Salesforce.

Il provider di identità deve inviare le asserzioni SAML a Salesforce utilizzando il profilo POST per Single Sign-On su browser Web SAML. Salesforce invia le risposte SAML all'`URL di accesso provider identità` specificato in Imposta immettendo *`Single Sign-On`* nella casella `Ricerca veloce` e selezionando **Impostazioni Single Sign-On**. Salesforce riceve l'asserzione, la verifica in base alla propria configurazione di Salesforce e, se l'asserzione risulta vera, consente il Single Sign-On.

In caso di problemi con l'asserzione SAML dopo la configurazione di Salesforce per SAML, utilizzare il Validatore asserzione SAML per convalidare l'asserzione SAML. Può essere necessario ottenere un'asserzione SAML dal proprio provider di identità.

Se gli utenti incontrano problemi utilizzando SAML per l'accesso, è possibile riesaminare la cronologia accessi SAML per stabilire il motivo del mancato accesso e condividere tale informazione con il provider di identità.

Se il proprio provider di identità supporta i metadati e se si è configurato SAML con la versione 2.0, è possibile fare clic su **Scarica metadati** per inviargli il file XML scaricato, che il provider può caricare per configurare automaticamente le sue impostazioni di connessione all'organizzazione o alla comunità Salesforce.

IN QUESTA SEZIONE:



EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

L'autenticazione federata è disponibile in: **tutte** le versioni

L'autenticazione delegata è disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

I provider di autenticazione sono disponibili nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:
- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:
- "Personalizza applicazione"

  E

  "Modifica tutti i dati"

## Utilizzo del provider di identità

1. È necessario raccogliere le seguenti informazioni dal provider di identità prima di configurare Salesforce per SAML.
   - La versione di SAML utilizzata dal provider di identità (1.1 o 2.0)
   - L'ID entità del provider di identità (denominato anche emittente)
   - Un certificato di autenticazione.

     Suggerimento: assicurarsi di memorizzare il certificato in una posizione accessibile dal browser. Tale certificato verrà poi caricato in Salesforce in una seconda fase.

   - I seguenti parametri dell'asserzione SAML, in base alle esigenze:
     - Tipo ID utente SAML
     - Posizione ID utente SAML
     - Nome attributo
     - URI attributo
     - Formato ID nome

     Nota: il Nome attributo, l'URI attributo e il Formato ID nome sono necessari solo se la `Posizione ID utente SAML` è un elemento dell'attributo e non l'elemento identificativo del nome di un'istruzione dell'oggetto

     Suggerimento: per impostare rapidamente il Single Sign-On, importare le impostazioni SAML 2.0 da un file XML (o da un URL che punta al file) nella pagina Impostazioni Single Sign-On. Ottenere l'XML dal provider di identità.

   È anche possibile condividere ulteriori informazioni su questi valori con il provider di identità.

   Suggerimento: abilitare Salesforce per SAML e acquisire una schermata della pagina per il provider di identità. Da Imposta, immettere *Impostazioni Single Sign-On* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni Single Sign-On**, fare clic su **Modifica** e selezionare `SAML abilitato`.

2. Lavorare con il provider di identità per configurare le pagine di avvio, accesso e disconnessione.
3. Condividere gli esempi di asserzioni SAML con il provider di identità per poter determinare il formato richiesto da Salesforce per un corretto Single Sign-On.

VEDERE ANCHE:

Informazioni su SAML

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

L'autenticazione federata è disponibile in: **tutte** le versioni

L'autenticazione delegata è disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

I provider di autenticazione sono disponibili nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:
- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:
- "Personalizza applicazione"

  E

  "Modifica tutti i dati"

## Configurazione delle impostazioni di SAML per Single Sign-On

Da questa pagina è possibile configurare l'organizzazione per l'utilizzo del Single Sign-On. È possibile anche impostare il provisioning just in time. Per configurare correttamente queste impostazioni, collaborare con il provider di identità. Per ulteriori informazioni su Single Sign-On, vedere Informazioni su Single Sign-On. Per ulteriori informazioni sul provisioning just in time, vedere Informazioni sul provisioning just in time.

Per configurare le impostazioni di SAML per il Single Sign-On dal provider di identità aziendale a Salesforce:

1. Raccogliere le informazioni dal provider di identità.
2. Fornire le informazioni al provider di identità.
3. Impostare Single Sign-On.
4. Impostare un provider di identità per crittografare le asserzioni SAML (facoltativo).
5. Abilitare il provisioning utente just in time (facoltativo).
6. Modificare l'handler just in time SAML se si è selezionato `Just in time SAML personalizzato con handler Apex` per il provisioning just in time.
7. Provare la connessione Single Sign-On.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

L'autenticazione federata è disponibile in: **tutte** le versioni

L'autenticazione delegata è disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

I provider di autenticazione sono disponibili nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:
- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:
- "Personalizza applicazione"

  E

  "Modifica tutti i dati"

### Impostare Single Sign-On

1. In Salesforce, da Imposta, immettere *`Impostazioni Single Sign-On`* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni Single Sign-On** e fare clic su **Modifica**.
2. Selezionare `SAML abilitato`. Per visualizzare le impostazioni di Single Sign-On SAML, è necessario abilitare SAML.
3. Specificare la versione di SAML utilizzata dal provider di identità.
4. Fare clic su **Salva**.
5. In Impostazioni Single Sign-On SAML, fare clic sul pulsante appropriato per creare una nuova configurazione, come illustrato di seguito.
   - **Nuova** - Specificare manualmente tutte le impostazioni.
   - **Nuova da file dei metadati** - Importare le impostazioni SAML 2.0 da un file XML fornito dal provider di identità. L'opzione legge il file XML e lo utilizza per specificare il maggior numero possibile di impostazioni.

     Nota: se il file XML contiene informazioni per più di una configurazione, viene usata la configurazione che ricorre per prima nel file XML.
   - **Nuova da URL dei metadati** - Importare le impostazioni SAML 2.0 da un URL pubblico. L'opzione legge il file XML accessibile da un URL pubblico e lo utilizza per specificare il maggior numero possibile di impostazioni. Per poter accedere all'URL dall'organizzazione Salesforce, è necessario aggiungerlo nelle Impostazioni sito remoto.
6. Assegnare a questa impostazione un **Nome** di riferimento all'interno dell'organizzazione.

   Salesforce inserisce il valore **Nome API** corrispondente, che se necessario si può personalizzare.
7. Immettere l'`Emittente`. Quest'ultimo viene spesso indicato come ID entità per il provider di identità.

8. Se nell'organizzazione Salesforce sono stati distribuiti i domini, indicare se si desidera utilizzare il dominio di base (`https://saml.salesforce.com`) o il dominio personalizzato per l'**ID entità**. Questa informazione deve essere condivisa con il provider di identità.

   Suggerimento: in genere come ID entità si utilizza il dominio personalizzato. Se Single Sign-On è già stato configurato prima della distribuzione di un dominio, il dominio di base è l'ID entità. Se si fornisce Salesforce ai servizi Salesforce, è necessario specificare il dominio personalizzato.

9. Per il `Certificato provider identità`, utilizzare il pulsante **Sfoglia** per trovare e caricare il certificato di autenticazione emesso dal provider di identità.
10. Per `Certificato di firma della richiesta`, selezionare il certificato desiderato fra quelli salvati nelle impostazioni **Gestione certificati e chiavi**.
11. Per il `Metodo di firma della richiesta`, selezionare l'algoritmo di hashing per le richieste crittografate, `RSA-SHA1` o `RSA-SHA256`.
12. Se il provider di identità crittografa le asserzioni SAML, è possibile selezionare il `Certificato decrittografia asserzione` usato dal provider da quelli salvati nelle impostazioni **Gestione certificati e chiavi**. Questo campo è disponibile solo se l'organizzazione supporta più configurazioni Single Sign-On. Per ulteriori informazioni, vedere Impostare un provider di identità per crittografare le asserzioni SAML.
13. Per `Tipo di identità SAML`, `Posizione identità SAML` e altri campi descritti in Valori dei provider di identità, specificare i valori forniti dal proprio provider di identità a seconda dei casi.
14. Per `Binding della richiesta avviata dal provider di servizi`, selezionare il valore appropriato in base alle informazioni fornite dal provider di identità.
15. Per SAML 2.0, se il provider di identità ha pagine di accesso o disconnessione specifiche, indicarle, rispettivamente, nei campi **URL di accesso provider identità** e **URL di disconnessione provider identità**.

    Nota: Questi campi compaiono per impostazione predefinita nelle organizzazioni Developer Edition e Sandbox e nelle organizzazioni di produzione solo se è abilitato Dominio personale. Non compaiono nelle organizzazioni di prova o nei Sandbox collegati a organizzazioni di prova.

16. Per `URL di errore personalizzato`, specificare l'URL della pagina a cui devono essere indirizzati gli utenti in caso di errore di accesso SAML. Deve essere una pagina accessibile pubblicamente, ad esempio una pagina Visualforce di un sito pubblico. L'URL può essere assoluto o relativo.
17. Se lo si desidera, impostare il provisioning utente just in time. Per ulteriori informazioni, vedere Abilitare il provisioning utente just in time e Informazioni sul provisioning just in time per SAML.
18. Fare clic su **Salva**.

Se il proprio provider di identità supporta i metadati e se si è configurato SAML con la versione 2.0, è possibile fare clic su **Scarica metadati** per inviargli il file XML scaricato, che il provider può caricare per configurare automaticamente le sue impostazioni di connessione all'organizzazione o alla comunità Salesforce.

## Impostare un provider di identità per crittografare le asserzioni SAML

Quando Salesforce è il provider di servizi per le asserzioni SAML in entrata, è possibile scegliere un certificato salvato per decrittografare le asserzioni in entrata di provider di identità terzi. È necessario fornire una copia di tale certificato al provider di identità.

1. Aggiungere una nuova configurazione SAML nella pagina Impostazioni Single Sign-On di Imposta.
2. Nel campo `Certificato decrittografia asserzione`, specificare il certificato da crittografare a partire da quelli salvati nelle impostazioni **Gestione certificati e chiavi**.

Nota: Se il campo `Certificato decrittografia asserzione` non è visualizzato è necessario abilitare più configurazioni Single Sign-On per l'organizzazione (questo vale per le organizzazioni create prima del rilascio Summer '13 che non utilizzano SAML 1.1). Per abilitare più configurazioni Single Sign-On, selezionare **Abilita config multiple** nella pagina **Impostazioni Single Sign-On**. Se questa impostazione è già stata abilitata, il campo è visualizzato e il pulsante **Abilita config multiple** non compare.

3. Impostare la `Posizione identità SAML` su `L'identità è nell'elemento NameIdentifier dell'istruzione dell'oggetto`.

   Affinché l'autenticazione vada a buon fine, l'utente deve essere identificato nell'istruzione `<Subject>` dell'asserzione. Per ulteriori informazioni, vedere Valori dei provider di identità.

4. Quando si salva la nuova configurazione SAML, il valore delle impostazioni SAML dell'organizzazione per l'`URL di accesso Salesforce` (noto anche come "URL ACS Salesforce") cambia. Indicare il nuovo valore (dalla pagina Impostazioni Single Sign-On di Imposta) e fare clic sul nome della nuova configurazione SAML. Il valore si trova nel campo `URL di accesso Salesforce`.
5. Il provider di identità deve utilizzare il valore `URL di accesso Salesforce`.
6. È necessario inoltre fornire al provider di identità una copia del certificato selezionato nel campo `Certificato decrittografia asserzione` da utilizzare per crittografare le asserzioni.

## Abilitare il provisioning utente just in time

1. In Impostazioni Single Sign-On SAML, selezionare `Provisioning utente abilitato`.
   - `Standard` - Questa opzione consente di eseguire automaticamente il provisioning degli utenti utilizzando gli attributi presenti nell'asserzione.
   - `Just in time SAML personalizzato con handler Apex` - Questa opzione esegue il provisioning degli utenti in base alla logica di una classe Apex.
2. Se si è selezionato `Standard`, fare clic su **Salva** e provare la connessione Single Sign-On.. Se si è selezionato `Just in time SAML personalizzato con handler Apex`, passare alla fase seguente.
3. Nel campo `Handler Just in time SAML`, selezionare una classe Apex esistente come classe di handler just in time SAML. La classe deve implementare l'interfaccia SamlJitHandler. In assenza di una classe Apex, è possibile generarne una facendo clic su `Crea automaticamente un modello di handler just in time SAML`. È necessario modificare questa classe e il contenuto predefinito prima di utilizzarlo. Per ulteriori informazioni, vedere Modifica dell'handler just in time SAML.
4. Nel campo `Esegui handler come`, selezionare l'utente che esegue la classe Apex. L'utente deve disporre dell'autorizzazione "Gestisci utenti".
5. Per il provisioning just in time è necessario un ID federazione nel tipo di utente. In `Tipo di identità SAML`, selezionare `L'asserzione contiene l'ID federazione dell'oggetto utente`. Se il provider di identità in precedenza utilizzava il nome utente Salesforce, comunicargli che deve utilizzare l'ID federazione.
6. Fare clic su **Salva**.

## Modificare l'handler just in time SAML

1. Da Imposta, immettere *`Classi Apex`* nella casella `Ricerca veloce`, quindi selezionare **Classi Apex**.
2. Modificare l'handler just in time SAML Apex generato per mappare i campi fra SAML e Salesforce. Inoltre, è possibile modificare il codice generato per supportare:
   - Campi personalizzati
   - Corrispondenza "fuzzy" dei profili

- Corrispondenza "fuzzy" dei ruoli
- Ricerca di referenti per email
- Ricerca di account per numero account
- Provisioning standard di utenti in una comunità
- Accesso standard degli utenti a una comunità
- Utilizzo dell'ID profilo predefinito per il provisioning just in time nei portali
- Utilizzo del ruolo portale predefinito per il provisioning just in time nei portali
- Generazione di nomi utente per il provisioning just in time nei portali

Ad esempio, per supportare i campi personalizzati nel codice generato per l'handler, trovare il commento "Handle custom fields here" nel codice generato. Inserire il codice del campo personalizzato dopo questo commento. Per ulteriori informazioni ed esempi, vedere la documentazione dell'interfaccia SamlJitHandler.

Nota: Se il proprio provider di identità invia gli attributi JIT per l'oggetto Referente o Account con l'oggetto Utente nella stessa asserzione, l'handler generato potrebbe non essere in grado di eseguire gli aggiornamenti. Per un elenco dei campi Utente che non possono essere aggiornati contemporaneamente ai campi Referente o Account, vedere sObject che non possono essere utilizzati insieme in operazioni DML.

## Provare la connessione Single Sign-On

Dopo aver configurato e salvato le proprie impostazioni SAML, testarle tentando di accedere all'applicazione del provider di identità. Il provider di identità indirizza il browser dell'utente all'INVIO (POST) di un modulo contenente le asserzioni SAML alla pagina di accesso Salesforce. Ogni asserzione viene verificata e, se corretta, viene consentito il Single Sign-On.

In caso di problemi di accesso utilizzando il Single Sign-On dopo avere configurato e salvato le impostazioni SAML, utilizzare il Validatore asserzione SAML. Può essere necessario ottenere preventivamente un'asserzione SAML dal proprio provider di identità.

Se gli utenti incontrano problemi utilizzando SAML per l'accesso, è possibile riesaminare la cronologia accessi SAML per stabilire il motivo del mancato accesso e condividere tale informazione con il provider di identità.

Se si utilizza SAML versione 2.0, al termine della configurazione di SAML, il campo Endpoint token OAuth 2.0 sarà compilato. Utilizzarlo con il flusso di autenticazione single sign-on per il Web di OAuth 2.0.

VEDERE ANCHE:

Informazioni su SAML

Procedure consigliate per l'implementazione di Single Sign-On

Convalida delle impostazioni SAML per single sign-on

Informazioni sui certificati e le chiavi Salesforce

## Visualizzazione delle impostazioni Single Sign-On

Dopo avere configurato l'organizzazione Salesforce in modo che utilizzi SAML, è possibile visualizzare le impostazioni single sign-on. Da Imposta, immettere *Impostazioni Single Sign-On* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni Single Sign-On**.

Questa pagina visualizza i dettagli della configurazione SAML. La maggior parte di questi campi sono gli stessi della pagina di configurazione SAML. I campi seguenti contengono informazioni generate automaticamente completando la configurazione. I campi disponibili dipendono dalla configurazione.

| Campo | Descrizione |
| --- | --- |
| `URL di accesso Salesforce` | Solo per SAML 2.0. Se si seleziona "L'asserzione contiene il nome utente Salesforce dell'utente" per il campo `Tipo ID utente SAML` e "L'ID utente è nell'elemento NameIdentifier dell'istruzione dell'oggetto" per `Posizione ID utente SAML`, questo URL è l'URL associato all'accesso per il flusso di asserzioni OAuth Single Sign-On per il Web. |
| `URL di disconnessione Salesforce` | Per SAML 2.0. Visualizza l'URL di disconnessione da Salesforce a cui viene indirizzato l'utente dopo la disconnessione. Questo URL viene utilizzato solo se non è specificato alcun valore per `URL di disconnessione provider identità`. |
| `Endpoint token OAuth 2.0` | Solo per SAML 2.0: l'URL ACS utilizzato per l'abilitazione di Salesforce come provider di identità nel flusso di asserzioni OAuth single sign-on per il Web. |

Da questa pagina è possibile effettuare una delle operazioni seguenti:

- Fare clic su **Modifica** per modificare la configurazione SAML esistente.
- Fare clic su **Validatore asserzione SAML** per convalidare le impostazioni SAML per la propria organizzazione utilizzando un'asserzione SAML fornita dal proprio provider di identità.
- Se il proprio provider di identità supporta i metadati e se si è configurato SAML con la versione 2.0, è possibile fare clic su **Scarica metadati** per inviargli il file XML scaricato, che il provider può caricare per configurare automaticamente le sue impostazioni di connessione all'organizzazione o alla comunità Salesforce.

VEDERE ANCHE:

Informazioni su SAML

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

L'autenticazione federata è disponibile in: **tutte** le versioni

L'autenticazione delegata è disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

I provider di autenticazione sono disponibili nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:
- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:
- "Personalizza applicazione"

  E

  "Modifica tutti i dati"

## Valori dei provider di identità

Prima di poter configurare Salesforce per SAML, è necessario ricevere le informazioni dal provider di identità. Tali informazioni devono essere utilizzate nella pagina di Single Sign-On.

Le informazioni riportate di seguito possono essere utili per il provider di identità.

| Campo | Descrizione |
| --- | --- |
| `Versione SAML` | La versione di SAML utilizzata dal provider di identità. Salesforce attualmente supporta la versione 1.1 e 2.0. Le specifiche SAML per le diverse versioni sono elencate di seguito con i rispettivi link:<br>• SAML 1.1<br>• SAML 2.0 |
| `Emittente` | L'ID entità, un URL che identifica in modo univoco il proprio provider di identità SAML. Le asserzioni SAML inviate a Salesforce devono corrispondere esattamente a questo valore nell'attributo `<saml:Issuer>` delle asserzioni SAML. |
| `ID entità` | L'emittente nelle richieste SAML generate da Salesforce nonché il pubblico previsto per qualsiasi Risposta SAML in arrivo. Se non sono stati distribuiti domini, questo valore è sempre `https://saml.salesforce.com`. Se sono stati distribuiti i domini, Salesforce consiglia di utilizzare il proprio nome dominio personalizzato. Per trovare il valore, andare alla pagina Impostazioni Single Sign-On. Da Imposta, immettere *Impostazioni Single Sign-On* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni Single Sign-On**. |
| `Certificato provider identità` | Il certificato di autenticazione emesso dal provider di identità. |
| `Certificato di firma della richiesta` | Il certificato (salvato nella pagina Gestione certificati e chiavi in Imposta) utilizzato per generare la firma su una richiesta SAML al provider di identità quando Salesforce è il provider di servizi per un accesso SAML avviato dal provider di servizi. Se un certificato non è stato salvato nella pagina Gestione certificati e chiavi in Imposta, Salesforce utilizza per impostazione predefinita il certificato proxy globale. L'uso di un certificato di firma salvato garantisce maggiore controllo sugli eventi, ad esempio sulla scadenza del certificato, rispetto all'uso del certificato proxy globale. |
| `Metodo di firma della richiesta` | L'algoritmo di hashing per le richieste crittografate, `RSA-SHA1` o `RSA-SHA256`. |

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

L'autenticazione federata è disponibile in: **tutte** le versioni

L'autenticazione delegata è disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

I provider di autenticazione sono disponibili nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:
- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:
- "Personalizza applicazione"

  E

  "Modifica tutti i dati"

| Campo | Descrizione |
| --- | --- |
| Tipo di identità SAML | L'elemento in un'asserzione SAML che contiene la stringa che identifica un utente Salesforce. I valori sono:<br>**L'asserzione contiene il nome utente Salesforce dell'utente**<br>Utilizzare questa opzione se il proprio provider di identità trasmette il nome utente Salesforce nelle asserzioni SAML.<br>**L'asserzione contiene l'ID federazione dell'oggetto utente**<br>Utilizzare questa opzione se il proprio provider di identità trasmette un ID utente esterno, ad esempio un ID dipendente, nell'asserzione SAML per identificare l'utente.<br>**L'asserzione contiene l'ID utente dell'oggetto utente**<br>Utilizzare questa opzione se il proprio provider di identità trasmette un ID utente interno, ad esempio un ID utente dell'organizzazione Salesforce, nell'asserzione SAML per identificare l'utente. |
| Posizione identità SAML | Il punto dell'asserzione nel quale viene identificato l'utente. I valori sono:<br>**L'identità è nell'elemento NameIdentifier dell'istruzione dell'oggetto**<br>L'elemento Username o FederationIdentifier di Salesforce si trova nell'istruzione <Subject> dell'asserzione.<br>**L'identità è un elemento Attribute**<br>L'elemento Username o FederationIdentifier di Salesforce è specificato nell'istruzione <AttributeValue>, che si trova nell'elemento <Attribute> dell'asserzione. |
| Nome attributo | Se è selezionato "L'identità è un elemento Attribute", contiene il valore di AttributeName specificato nell'elemento <Attribute> che contiene l'ID utente. |
| URI attributo | Se SAML 1.1 è la versione SAML specificata ed è selezionato "L'identità è un elemento Attribute", contiene il valore di AttributeNamespace specificato in <Attribute>. |
| Formato ID nome | Se SAML 2.0 è la versione SAML specificata ed è selezionato "L'identità è un elemento Attribute", contiene il valore di nameid-format. I valori possibili includono unspecified, emailAddress o persistent. Tutti i valori validi sono contenuti nella sezione "Name Identifier Format Identifiers" del documento Assertions and Protocols SAML 2.0 specification. |
| Binding della richiesta avviata dal provider di servizi | Se si utilizza Dominio personale, scegliere il metodo di binding richiesto dal provider di identità per i messaggi SAML. I valori sono:<br>**POST HTTP**<br>Il binding POST HTTP invia i messaggi SAML utilizzando moduli HTML con codifica base64.<br>**Reindirizzamento HTTP**<br>Il binding Reindirizzamento HTTP invia i messaggi SAML con codifica base64 e URL all'interno dei parametri URL.<br>Indipendentemente dal binding di richiesta selezionato, la risposta SAML utilizza sempre il binding POST HTTP. |
| URL di accesso provider identità | Solo per SAML 2.0: URL in cui Salesforce invia una richiesta SAML per avviare la sequenza di accesso.<br>Se sono stati distribuiti i domini e in questo campo viene specificato un valore, le richieste di accesso vengono solitamente inviate all'indirizzo specificato in questo campo. Se invece si desidera ignorare |

| Campo | Descrizione |
| --- | --- |
| | questo valore (ad esempio quando il provider di identità non è attivo), aggiungere il parametro `login` alla stringa di query per la pagina di accesso. Ad esempio: `http://mydomain.my.salesforce.com?login`.<br>Nota: questo campo compare per impostazione predefinita nelle organizzazioni Developer Edition di produzione e Sandbox e nelle organizzazioni di produzione solo se è abilitato Dominio personale. Non compare nelle organizzazioni di prova o nei Sandbox collegati a organizzazioni di prova. |
| `URL di disconnessione provider identità` | Solo per SAML 2.0: URL a cui indirizzare l'utente quando fa clic sul link **Esci** in Salesforce. L'impostazione predefinita è `http://www.salesforce.com`.<br>Nota: questo campo compare per impostazione predefinita nelle organizzazioni Developer Edition di produzione e Sandbox e nelle organizzazioni di produzione solo se è abilitato Dominio personale. Non compare nelle organizzazioni di prova o nei Sandbox collegati a organizzazioni di prova. |
| `URL di accesso Salesforce` | URL associato all'accesso per il flusso Single Sign-On del browser Web. |
| `Endpoint token OAuth 2.0` | Solo per SAML 2.0: URL ACS utilizzato con l'API per l'abilitazione di Salesforce come provider di identità nel flusso di asserzioni OAuth Single Sign-On per il Web. |
| `URL di errore personalizzato` | URL della pagina a cui devono essere indirizzati gli utenti se si verifica un errore durante l'accesso SAML. Deve essere una pagina accessibile pubblicamente, ad esempio una pagina Visualforce di un sito pubblico. L'URL può essere assoluto o relativo. |

## Valori degli URL di avvio, accesso e disconnessione

Oltre alle informazioni utilizzate durante il single sign-on, il provider di identità può anche impostare le pagine di avvio, accesso e disconnessione. Queste pagine possono anche essere impostate dall'utente durante la configurazione di single sign-on.

Le informazioni riportate di seguito possono essere utili per il provider di identità durante l'impostazione di queste pagine.

- La specifica SAML supporta un modulo HTML utilizzato per trasmettere l'asserzione SAML tramite POST HTTPS.
- Per SAML 1.1, il provider di identità SAML può incorporare coppie nome-valore nel campo `TARGET` per passare queste informazioni aggiuntive a Salesforce sotto forma di prefisso con un URL formattato appositamente che contiene parametri codificati nell'URL.
- L'URL per SAML 1.1 da includere nel campo `TARGET` è il seguente: `https://saml.salesforce.com/?`
- Per SAML 2.0, invece di utilizzare il campo `TARGET`, il provider di identità utilizza `<AttributeStatement>` nell'asserzione SAML per specificare le informazioni aggiuntive.
- Salesforce supporta i seguenti parametri:

  Nota: Per SAML 1.1 questi parametri devono essere codificati nell'URL. Questo consente una corretta gestione degli URL che vengono trasmessi come valori che includono parametri propri. Per SAML 2.0 questi parametri fanno parte di `<AttributeStatement>`.

  - `ssoStartPage` è la pagina alla quale l'utente deve essere reindirizzato quando tenta di accedere con SAML. L'utente viene indirizzato a questa pagina quando richiede una risorsa protetta in Salesforce senza una sessione attiva. `ssoStartPage` deve essere la pagina di accesso del provider di identità SAML.

- `startURL` è l'URL al quale indirizzare l'utente quando il sign-on viene completato con successo. L'URL può essere in formato assoluto, come *`https://na1.salesforce.com/001/o`* o relativo, ad esempio *`/001/o`*. Questo parametro è utilizzato solo in SAML 1.1. In SAML 2.0, l'URL iniziale è la pagina alla quale l'utente ha tentato di accedere prima di essere autenticato.
- `logoutURL` è l'URL a cui indirizzare l'utente quando fa clic sul link **Disconnetti** in Salesforce. L'impostazione predefinita è `http://www.salesforce.com`.

Il seguente esempio di campo `TARGET` è destinato a SAML 1.1 e comprende parametri codificati correttamente. Passa una pagina iniziale personalizzata, oltre agli URL iniziale e di disconnessione incorporati come valori di parametro nella stringa di query.

```
https://saml.salesforce.com/?ssoStartPage=https%3A%2F
%2Fwww.customer.org%2Flogin%2F&startURL=%2F001%2Fo&logoutURL=http%3A%2F%2Fwww.salesforce.com
```

Segue un esempio di `<AttributeStatement>` per SAML 2.0 contenente sia `ssoStartPage` che `logoutURL`:

```
<saml:AttributeStatement>
   <saml:Attribute Name="ssoStartPage"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
           xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:anyType">
              http://www.customer.org
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="logoutURL"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
           xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">
              https://www.salesforce.com
      </saml:AttributeValue>
   </saml:Attribute>
</saml:AttributeStatement>
```

VEDERE ANCHE:

Informazioni su SAML

## Personalizzazione delle pagine di avvio, errore, accesso e disconnessione di SAML

Per gli utenti con Single Sign-On che utilizzano SAML 1.1 o 2.0 è possibile personalizzare le pagine di avvio, errore, accesso e disconnessione. Nell'ambito della propria configurazione, decidere le seguenti impostazioni:

- Se il proprio provider di identità utilizza SAML 1.1, l'URL a cui indirizzare l'utente quando viene eseguito correttamente il Single Sign-On (pagina di avvio). L'URL può essere in formato assoluto, come `https://na1.salesforce.com/001/o` o relativo, ad esempio `/001/o`. Questo URL deve essere un endpoint che accetta le richieste di autenticazione SAML.

  In SAML 2.0, la pagina di avvio è la pagina alla quale l'utente ha tentato di accedere prima di essere autenticato. La pagina di avvio SAML 2.0 deve supportare il Single Sign-On Sp-init.

  Se si utilizza SAML 2.0 è possibile anche utilizzare il parametro `RelayState` per controllare l'indirizzo a cui vengono reindirizzati gli utenti quando l'accesso viene completato correttamente.

- La pagina di avvio di single sign-on dove Salesforce invia una richiesta SAML per iniziare la sequenza di accesso.

  Se si specifica una pagina di avvio per Single Sign-On, si consiglia di specificare anche una pagina di disconnessione. Se si specifica una pagina di disconnessione, quando un utente fa clic sull'opzione di disconnessione o la sua sessione scade, viene reindirizzato a quella pagina. Se non viene specificata una pagina di disconnessione, l'utente viene reindirizzato alla pagina di accesso generale di Salesforce.

- L'URL a cui indirizzare l'utente quando fa clic sul link Esci in Salesforce (pagina di disconnessione). L'impostazione predefinita è `https://login.salesforce.com`, a meno che non sia abilitato Dominio personale. Se è abilitato Dominio personale, l'impostazione predefinita è `https://`*`dominiopersonale`*`.my.salesforce.com`.

Per SAML 2.0, questi valori possono essere impostati durante la configurazione di single sign-on oppure dal provider di identità nell'URL di accesso o nell'asserzione SAML. L'ordine di precedenza è il seguente:

1. Cookie sessione: se si è già effettuato l'accesso a Salesforce ed esiste ancora un cookie, vengono utilizzate le pagine di accesso e di disconnessione specificate dal cookie della sessione.
2. Valori trasmessi dal provider di identità.
3. Valori dalla pagina di configurazione di single sign-on.

Se si decide di non aggiungere questi valori alla configurazione single sign-on, condividerli con il provider di identità. Il provider di identità deve utilizzare questi valori nell'URL di accesso o nell'asserzione.

Si può anche decidere se gli utenti dovranno essere indirizzati a una pagina di errore personalizzata se si verifica un errore durante l'accesso SAML: deve essere una pagina accessibile pubblicamente, ad esempio una pagina Visualforce di un sito pubblico. L'URL può essere assoluto o relativo. Utilizzare questo valore quando si configura SAML.

VEDERE ANCHE:

Informazioni su SAML

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

L'autenticazione federata è disponibile in: **tutte** le versioni

L'autenticazione delegata è disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

I provider di autenticazione sono disponibili nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:

- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:

- "Personalizza applicazione"

  E

  "Modifica tutti i dati"

## Esempi di asserzioni SAML

Condividere le asserzioni SAML di esempio con il provider di identità per poter determinare il formato delle informazioni richieste da Salesforce per un corretto Single Sign-On. L'asserzione deve essere firmata in base alla specifica XML Signature, utilizzando RSA e SHA-1 o SHA-256.

Oltre agli esempi generici di Single Sign-On sia per SAML 1.1 che per SAML 2.0, utilizzare gli esempi che seguono per le singole funzioni specifiche:

- asserzioni per i portali
- asserzioni per i Siti
- messaggio SOAP per l'autenticazione delegata
- asserzione per il provisioning just in time

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

L'autenticazione federata è disponibile in: **tutte** le versioni

L'autenticazione delegata è disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

I provider di autenticazione sono disponibili nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:
- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:
- "Personalizza applicazione"

  E

  "Modifica tutti i dati"

**Il tipo di ID utente SAML è il nome utente Salesforce e il percorso dell'ID utente SAML è l'elemento `<NameIdentifier>` nell'elemento `<Subject>`**

SAML 1.1:

```
<Subject>
      <NameIdentifier>user101@salesforce.com</NameIdentifier>
</Subject>
```

SAML 2.0:

```
<saml:Subject>
    <saml:NameID
```

```
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">user101@salesforce.com</saml:NameID>

    <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <saml:SubjectConfirmationData NotOnOrAfter="2008-06-26T02:44:24.173Z"
Recipient="http://localhost:9000"/>
    </saml:SubjectConfirmation>
</saml:Subject>
```

**Il tipo di ID utente SAML è il nome utente Salesforce e la posizione dell'ID utente SAML è l'elemento `<Attribute>`**

SAML 1.1:

```
<AttributeStatement>
    <Subject>
      <NameIdentifier>this value doesn't matter</NameIdentifier>
         <SubjectConfirmation>
          <ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</ConfirmationMethod>

    </SubjectConfirmation>
 </Subject>
    <Attribute AttributeName="MySfdcName" AttributeNamespace="MySfdcURI">
       <AttributeValue>user101@salesforce.com</AttributeValue>
 </Attribute>
    </AttributeStatement>
```

SAML 2.0:

```
<saml:AttributeStatement>
    <saml:Attribute FriendlyName="fooAttrib" Name="SFDC_USERNAME"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
        <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">
            user101@salesforce.com
        </saml:AttributeValue>
    </saml:Attribute>
 </saml:AttributeStatement>
```

**Il tipo di ID utente SAML è il campo `FederationIdentifier` dell'oggetto utente Salesforce, mentre la posizione dell'ID utente SAML è l'elemento `<NameIdentifier>` nell'elemento `<Subject>`.**

SAML 1.1:

```
<AttributeStatement>
   <saml:Subject>
      <saml:NameIdentifier Format="urn:oasis:names:tc:SAML:1.0:assertion"
NameQualifier="www.saml_assertions.com">
         MyName
      </saml:NameIdentifier>
   </saml:Subject>
</AttributeStatement>
```

SAML 2.0:

```
<saml:Subject>
    <saml:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">MyName</saml:NameID>
    <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <saml:SubjectConfirmationData NotOnOrAfter="2008-06-26T02:48:25.730Z"
```

```
Recipient="http://localhost:9000/"/>
    </saml:SubjectConfirmation>
</saml:Subject>
```

Nota: L'identificatore del nome può essere una qualsiasi stringa arbitraria, inclusi gli indirizzi email e le stringhe ID numeriche.

**Il tipo di ID utente SAML è il campo `FederationIdentifier` dell'oggetto utente Salesforce, mentre la posizione dell'ID utente SAML è l'elemento `<Attribute>`.**

SAML 1.1:

```
<AttributeStatement>
    <Subject>
      <NameIdentifier>who cares</NameIdentifier>
         <SubjectConfirmation>
          <ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</ConfirmationMethod>

    </SubjectConfirmation>
 </Subject>
    <Attribute AttributeName="MyName" AttributeNamespace="MyURI">
       <AttributeValue>user101</AttributeValue>
 </Attribute>
    </AttributeStatement>
```

SAML 2.0:

```
<saml:AttributeStatement>
    <saml:Attribute FriendlyName="fooAttrib" Name="SFDC_ATTR"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
        <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">
            user101
        </saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

**Il tipo di ID utente SAML è il nome utente Salesforce e il percorso dell'ID utente SAML è l'elemento `<NameIdentifier>` nell'elemento `<Subject>`**

Di seguito è riportata una risposta SAML completa, per SAML 2.0:

```
<samlp:Response ID="_257f9d9e9fa14962c0803903a6ccad931245264310738"
   IssueInstant="2009-06-17T18:45:10.738Z" Version="2.0">
<saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
   https://www.salesforce.com
</saml:Issuer>

<samlp:Status>
   <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
</samlp:Status>

<saml:Assertion ID="_3c39bc0fe7b13769cab2f6f45eba801b1245264310738"
   IssueInstant="2009-06-17T18:45:10.738Z" Version="2.0">
   <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
      https://www.salesforce.com
   </saml:Issuer>
```

```
   <saml:Signature>
      <saml:SignedInfo>
         <saml:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <saml:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>

         <saml:Reference URI="#_3c39bc0fe7b13769cab2f6f45eba801b1245264310738">
            <saml:Transforms>
               <saml:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
               <saml:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                  <ec:InclusiveNamespaces PrefixList="ds saml xs"/>
               </saml:Transform>
            </saml:Transforms>
            <saml:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <saml:DigestValue>vzR9Hfp8d16576tEDeq/zhpmLoo=
            </saml:DigestValue>
         </saml:Reference>
      </saml:SignedInfo>
      <saml:SignatureValue>
         AzID5hhJeJlG2llUDvZswNUrlrPtR7S37QYH2W+Un1n8c6kTC
         Xr/lihEKPcA2PZt86eBntFBVDWTRlh/W3yUgGOqQBJMFOVbhK
         M/CbLHbBUVT5TcxIqvsNvIFdjIGNkf1W0SBqRKZOJ6tzxCcLo
         9dXqAyAUkqDpX5+AyltwrdCPNmncUM4dtRPjI05CL1rRaGeyX
         3kkqOL8p0vjm0fazU5tCAJLbYuYgU1LivPSahWNcpvRSlCI4e
         Pn2oiVDyrcc4et12inPMTc2lGIWWWWJyHOPSiXRSkEAIwQVjf
         Qm5cpli44Pv8FCrdGWpEE0yXsPBvDkM9jIzwCYGG2fKaLBag==
      </saml:SignatureValue>
      <saml:KeyInfo>
         <saml:X509Data>
            <saml:X509Certificate>
               MIIEATCCAumgAwIBAgIBBTANBgkqhkiG9w0BAQ0FADCBgzELM
               [Certificate truncated for readability...]
            </saml:X509Certificate>
         </saml:X509Data>
      </saml:KeyInfo>
   </saml:Signature>

   <saml:Subject>
      <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">
         saml01@salesforce.com
      </saml:NameID>

      <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml:SubjectConfirmationData NotOnOrAfter="2009-06-17T18:50:10.738Z"
         Recipient="https://login.www.salesforce.com"/>
      </saml:SubjectConfirmation>
   </saml:Subject>

   <saml:Conditions NotBefore="2009-06-17T18:45:10.738Z"
      NotOnOrAfter="2009-06-17T18:50:10.738Z">

      <saml:AudienceRestriction>
         <saml:Audience>https://saml.salesforce.com</saml:Audience>
```

```
      </saml:AudienceRestriction>
   </saml:Conditions>

   <saml:AuthnStatement AuthnInstant="2009-06-17T18:45:10.738Z">
      <saml:AuthnContext>
         <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
         </saml:AuthnContextClassRef>
      </saml:AuthnContext>
   </saml:AuthnStatement>

   <saml:AttributeStatement>

      <saml:Attribute Name="portal_id">
         <saml:AttributeValue xsi:type="xs:anyType">060D00000000SHZ
         </saml:AttributeValue>
      </saml:Attribute>

      <saml:Attribute Name="organization_id">
         <saml:AttributeValue xsi:type="xs:anyType">00DD0000000F7L5
         </saml:AttributeValue>
      </saml:Attribute>

      <saml:Attribute Name="ssostartpage"
         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">

         <saml:AttributeValue xsi:type="xs:anyType">
            http://www.salesforce.com/security/saml/saml20-gen.jsp
         </saml:AttributeValue>
      </saml:Attribute>

      <saml:Attribute Name="logouturl"
         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">

         <saml:AttributeValue xsi:type="xs:string">
            http://www.salesforce.com/security/del_auth/SsoLogoutPage.html
         </saml:AttributeValue>
      </saml:Attribute>
   </saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>
```

## Esempi di asserzioni SAML per i portali

Di seguito sono illustrati gli attributi `portal_id` e `organization_id` in un'istruzione di asserzione SAML:

```
<saml:AttributeStatement>
   <saml:Attribute Name="portal_id">
      <saml:AttributeValue xsi:type="xs:anyType">060D00000000SHZ</saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="organization_id">
         <saml:AttributeValue xsi:type="xs:anyType">00DD0000000F7P5</saml:AttributeValue>
```

```
   </saml:Attribute>
</saml:AttributeStatement>
```

Di seguito viene riportata una dichiarazione di asserzione SAML completa che può essere utilizzata per il Single Sign-On per i portali. L'organizzazione utilizza il Single Sign-On federato, che viene incluso in un attributo (vedere il `<saml:AttributeStatement>` in grassetto nell'asserzione) e non nel subject.

```
<samlp:Response ID="_f97faa927f54ab2c1fef230eee27cba21245264205456"
      IssueInstant="2009-06-17T18:43:25.456Z" Version="2.0">
   <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
      https://www.salesforce.com</saml:Issuer>

   <samlp:Status>
      <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
   </samlp:Status>

   <saml:Assertion ID="_f690da2480a8df7fcc1cbee5dc67dbbb1245264205456"
      IssueInstant="2009-06-17T18:45:10.738Z" Version="2.0">
      <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
         https://www.salesforce.com
      </saml:Issuer>

      <saml:Signature>
         <saml:SignedInfo>
            <saml:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
           <saml:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>

            <saml:Reference URI="#_f690da2480a8df7fcc1cbee5dc67dbbb1245264205456">
               <saml:Transforms>
                  <saml:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                  <saml:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                     <ec:InclusiveNamespaces PrefixList="ds saml xs"/>
                  </saml:Transform>
               </saml:Transforms>
               <saml:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
               <saml:DigestValue>vzR9Hfp8d16576tEDeq/zhpmLoo=
               </saml:DigestValue>
            </saml:Reference>
         </saml:SignedInfo>
         <saml:SignatureValue>
            AzID5hhJeJlG2llUDvZswNUrlrPtR7S37QYH2W+Un1n8c6kTC
            Xr/lihEKPcA2PZt86eBntFBVDWTRlh/W3yUgGOqQBJMFOVbhK
            M/CbLHbBUVT5TcxIqvsNvIFdjIGNkf1W0SBqRKZOJ6tzxCcLo
            9dXqAyAUkqDpX5+AyltwrdCPNmncUM4dtRPjI05CL1rRaGeyX
            3kkqOL8p0vjm0fazU5tCAJLbYuYgU1LivPSahWNcpvRSlCI4e
            Pn2oiVDyrcc4et12inPMTc2lGIWWWWJyHOPSiXRSkEAIwQVjf
            Qm5cpli44Pv8FCrdGWpEE0yXsPBvDkM9jIzwCYGG2fKaLBag==
         </saml:SignatureValue>
         <saml:KeyInfo>
            <saml:X509Data>
               <saml:X509Certificate>
                  MIIEATCCAumgAwIBAgIBBTANBgkqhkiG9w0BAQ0FADCBgzELM
                  Certificate truncated for readability...
```

```
         </saml:X509Certificate>
      </saml:X509Data>
   </saml:KeyInfo>
</saml:Signature>

<saml:Subject>
   <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">null

   </saml:NameID>

   <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
   <saml:SubjectConfirmationData NotOnOrAfter="2009-06-17T18:48:25.456Z"
      Recipient="https://www.salesforce.com/?saml=02HKiPoin4f49GRMsOdFmhTgi
      _0nR7BBAflopdnD3gtixujECWpxr9klAw"/>
      </saml:SubjectConfirmation>
</saml:Subject>

<saml:Conditions NotBefore="2009-06-17T18:43:25.456Z"
   NotOnOrAfter="2009-06-17T18:48:25.456Z">

   <saml:AudienceRestriction>
      <saml:Audience>https://saml.salesforce.com</saml:Audience>
   </saml:AudienceRestriction>
</saml:Conditions>

<saml:AuthnStatement AuthnInstant="2009-06-17T18:43:25.456Z">

   <saml:AuthnContext>
      <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified

      </saml:AuthnContextClassRef>
   </saml:AuthnContext>
</saml:AuthnStatement>

<saml:AttributeStatement>

   <saml:Attribute FriendlyName="Friendly Name" Name="federationId"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:string">saml_portal_user_federation_id
      </saml:AttributeValue>
      <saml:AttributeValue xsi:type="xs:string">SomeOtherValue
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="portal_id">
      <saml:AttributeValue xsi:type="xs:anyType">060D00000000SHZ
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="organization_id">
      <saml:AttributeValue xsi:type="xs:anyType">00DD0000000F7Z5
      </saml:AttributeValue>
   </saml:Attribute>
```

```
         <saml:Attribute Name="ssostartpage"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">

            <saml:AttributeValue xsi:type="xs:anyType">
               http://www.salesforce.com/qa/security/saml/saml20-gen.jsp
            </saml:AttributeValue>
         </saml:Attribute>

         <saml:Attribute Name="logouturl"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">

            <saml:AttributeValue xsi:type="xs:string">
                http://www.salesforce.com/qa/security/del_auth/SsoLogoutPage.html
            </saml:AttributeValue>
         </saml:Attribute>
      </saml:AttributeStatement>
   </saml:Assertion>
</samlp:Response>
```

## Esempio di asserzione SAML per i Siti

Di seguito sono illustrati gli attributi `portal_id organization_id` e `siteurl` in un'istruzione di asserzione SAML:

```
<saml:AttributeStatement>
   <saml:Attribute Name="portal_id">
      <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:type="xs:anyType">060900000004cDk
      </saml:AttributeValue>
   </saml:Attribute>
   <saml:Attribute Name="organization_id">
      <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:type="xs:anyType">00D900000008bX0
      </saml:AttributeValue></saml:Attribute>
   <saml:Attribute Name="siteurl">
      <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:type="xs:anyType">https://ap1.force.com/mySuffix</saml:AttributeValue>
   </saml:Attribute>
</saml:AttributeStatement>
```

## Esempio di messaggio SOAP per l'autenticazione delegata

Nell'ambito della procedura di single sign-on mediante autenticazione delegata, il server di Salesforce esegue una richiesta SOAP 1.1 per autenticare l'utente che trasmette le credenziali. Segue un esempio di questo tipo di richiesta. Il servizio Web di single sign-on deve accettare questa richiesta, elaborarla e restituire una risposta di tipo `true` o `false`.

**Esempio di richiesta**

```
<?xml version="1.0" encoding="UTF-8" ?>
<soapenv:Envelope
   xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
   <soapenv:Body>
```

```
      <Authenticate xmlns="urn:authentication.soap.sforce.com">
         <username>sampleuser@sample.org</username>
         <password>myPassword99</password>
         <sourceIp>1.2.3.4</sourceIp>
      </Authenticate>
   </soapenv:Body>
</soapenv:Envelope>
```

**Esempio di messaggio di risposta**

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
   xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
   <soapenv:Body>
      <AuthenticateResult xmlns="urn:authentication.soap.sforce.com">
         <Authenticated>false</Authenticated>
      </AuthenticateResult>
   </soapenv:Body>
</soapenv:Envelope>
```

## Esempio di asserzione SAML per il provisioning just in time

Di seguito è riportata un'asserzione SAML di esempio per il provisioning just in time.

```
<saml:AttributeStatement>

   <saml:Attribute Name="User.Username"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">testuser@123.org
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="User.Phone"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">415-123-1234
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="User.FirstName"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">Testuser
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="User.LanguageLocaleKey"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">en_US
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="User.CompanyName"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">Salesforce.com
      </saml:AttributeValue>
   </saml:Attribute>
```

```
<saml:Attribute Name="User.Alias"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
   <saml:AttributeValue xsi:type="xs:anyType">tlee2
   </saml:AttributeValue>
</saml:Attribute>

<saml:Attribute Name="User.CommunityNickname"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
   <saml:AttributeValue xsi:type="xs:anyType">tlee2
   </saml:AttributeValue>
</saml:Attribute>

<saml:Attribute Name="User.UserRoleId"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
   <saml:AttributeValue xsi:type="xs:anyType">000000000000000
   </saml:AttributeValue>
</saml:Attribute>

<saml:Attribute Name="User.Title"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
   <saml:AttributeValue xsi:type="xs:anyType">Mr.
   </saml:AttributeValue>
</saml:Attribute>

<saml:Attribute Name="User.LocaleSidKey"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
   <saml:AttributeValue xsi:type="xs:anyType">en_CA
   </saml:AttributeValue>
</saml:Attribute>

<saml:Attribute Name="User.Email"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
   <saml:AttributeValue xsi:type="xs:anyType">testuser@salesforce.com
   </saml:AttributeValue>
</saml:Attribute>

<saml:Attribute Name=" User.FederationIdentifier"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
   <saml:AttributeValue xsi:type="xs:anyType">tlee2
   </saml:AttributeValue>
</saml:Attribute>

<saml:Attribute Name="User.TimeZoneSidKey"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
   <saml:AttributeValue xsi:type="xs:anyType">America/Los_Angeles
   </saml:AttributeValue>
</saml:Attribute>

<saml:Attribute Name="User.LastName"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
   <saml:AttributeValue xsi:type="xs:anyType">Lee
   </saml:AttributeValue>
</saml:Attribute>
```

```
   <saml:Attribute Name="User.ProfileId"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">00ex0000001pBNL
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="User.IsActive"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">1
      </saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name="User.EmailEncodingKey"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">UTF-8
      </saml:AttributeValue>
   </saml:Attribute>

</saml:AttributeStatement>
```

VEDERE ANCHE:

Informazioni su SAML

## Riesame della cronologia accessi SAML

Quando un utente accede a Salesforce da un'altra applicazione mediante single sign-on, le asserzioni SAML vengono inviate alla pagina di accesso Salesforce. Le asserzioni vengono confrontate con le asserzioni del certificato di autenticazione specificate nella pagina Impostazioni Single Sign-On di Imposta. Se l'accesso di un utente non riesce, nel registro della cronologia accessi viene riportato un messaggio che indica le ragioni per cui l'accesso non è riuscito. Inoltre, il Validatore asserzione SAML può essere automaticamente compilato con l'asserzione non valida.

Per visualizzare la cronologia degli accessi, da Imposta immettere *Cronologia accessi* nella casella Ricerca veloce, quindi selezionare **Cronologia accessi**. Dopo aver visualizzato la cronologia degli accessi, è possibile condividere le informazioni con il provider di identità.

Sono possibili i seguenti errori:

**Asserzione scaduta**

Il timestamp di un'asserzione è più vecchio di cinque minuti.

Nota: Salesforce ammette una differenza oraria di tre minuti. Ciò significa che, in pratica, un'asserzione può avere superato il timestamp da otto minuti o avere ancora tre minuti di validità. Questo tempo può essere inferiore se il periodo di validità dell'asserzione è minore di cinque minuti.

**Asserzione non valida**

Un'asserzione non è valida; ad esempio l'elemento <Subject> di un'asserzione può essere assente.

**Pubblico non valido**

Il valore specificato in <Audience> deve essere https://saml.salesforce.com.

**Errore di configurazione/autorizzazione disabilitata**

È stato rilevato un errore nella configurazione SAML in Salesforce. È possibile che il certificato caricato sia danneggiato o che la preferenza dell'organizzazione sia stata disabilitata. Per controllare la configurazione, da Imposta immettere *Impostazioni Single Sign-On* nella casella Ricerca veloce, quindi selezionare **Impostazioni Single Sign-On**. Quindi, prendere un'asserzione SAML di esempio dal provider di identità e fare clic su **Validatore asserzione SAML**.

**Mancata corrispondenza emittente**

L'emittente o l'ID entità specificato nell'asserzione non corrisponde a quello specificato nella configurazione Salesforce.

**Mancata corrispondenza destinatario**

Il destinatario specificato in un'asserzione non corrisponde a quello specificato nella configurazione Salesforce.

**Rilevato duplicato**

Lo stesso ID asserzione è stato usato più di una volta. Gli ID asserzione devono essere univoci all'interno dell'organizzazione.

**Firma non valida**

La firma in un'asserzione non è stata convalidata dal certificato nella configurazione Salesforce.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

L'autenticazione federata è disponibile in: **tutte** le versioni

L'autenticazione delegata è disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

I provider di autenticazione sono disponibili nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:
- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:
- "Personalizza applicazione"

  E

  "Modifica tutti i dati"

**Errore di conferma oggetto**

L'oggetto `<Subject>` specificato nell'asserzione non corrisponde alla configurazione di SAML presente in Salesforce.

VEDERE ANCHE:

Informazioni su SAML

## Convalida delle impostazioni SAML per single sign-on

Se gli utenti incontrano difficoltà per accedere a Salesforce dopo che si è configurato Salesforce per il Single Sign-On, utilizzare il Validatore asserzione SAML e la cronologia degli accessi per convalidare le asserzioni SAML inviate dal provider di identità.

1. Ottenere un'asserzione SAML per abilitare il proprio provider di identità. Questa asserzione può essere in formato XML normale o base64.

   Se un utente cerca di accedere a Salesforce senza riuscirci, l'asserzione SAML non valida viene utilizzata per compilare automaticamente il Validatore asserzione SAML, ove possibile.

2. Da Imposta, immettere *Impostazioni Single Sign-On* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni Single Sign-On** e fare clic su **Validatore asserzione SAML**.
3. Modificare l'asserzione SAML nella casella di testo, quindi fare clic su **Convalida**.
4. Condividere i risultati degli errori di convalida con il proprio provider di identità.

VEDERE ANCHE:

Informazioni su SAML

Informazioni su Single Sign-On

Procedure consigliate per l'implementazione di Single Sign-On

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

L'autenticazione federata è disponibile in: **tutte** le versioni

L'autenticazione delegata è disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

I provider di autenticazione sono disponibili nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:
- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:
- "Personalizza applicazione"

  E

  "Modifica tutti i dati"

## Errori di convalida asserzione SAML

Salesforce impone i seguenti requisiti di validità sulle asserzioni:

**Istruzione di autenticazione**

Il provider di identità deve includere un elemento `<AuthenticationStatement>` nell'asserzione.

**Istruzione di condizioni**

Se l'asserzione contiene un'istruzione `<Conditions>`, deve contenere un timestamp valido.

**Timestamp**

Il periodo di validità specificato in un'asserzione deve essere rispettato. Inoltre, il timestamp dell'asserzione deve risalire a meno di 5 minuti prima (con una tolleranza di tre minuti in più o in meno) indipendentemente dall'impostazione del periodo di validità dell'asserzione. Questo consente di tenere in considerazione le eventuali differenze di orario tra computer. Anche le limitazioni `NotBefore` e `NotOnOrAfter` devono essere definite e valide.

**Attributo**

Se la configurazione di Salesforce è impostata su `L'identità è un elemento Attribute`, l'asserzione del provider di identità deve contenere un elemento `<AttributeStatement>`.

Se si utilizza SAML 1.1, sia `<AttributeName>` che `<AttributeNamespace>` sono richiesti come parte di `<AttributeStatement>`.

Se si utilizza SAML 2.0, è richiesto solo `<AttributeName>`.

**Formato**

L'attributo `Format` di un'istruzione `<Issuer>` deve essere impostato su `"urn:oasis:names:tc:SAML:2.0:nameid-format:entity"` oppure non deve essere impostato.

Ad esempio:

```
<saml:Issuer
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://www.salesforce.com</saml:Issuer>
```

È valido anche l'esempio seguente:

```
<saml:Issuer >https://www.salesforce.com</saml:Issuer>
```

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

L'autenticazione federata è disponibile in: **tutte** le versioni

L'autenticazione delegata è disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

I provider di autenticazione sono disponibili nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:

- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:

- "Personalizza applicazione"

  E

  "Modifica tutti i dati"

**Emittente**

L'emittente specificato in un'asserzione deve corrispondere all'emittente specificato in Salesforce.

**Oggetto**

L'oggetto dell'asserzione deve essere risolto in modo che sia il nome utente Salesforce o l'ID federazione dell'utente.

**Pubblico**

Il valore `<Pubblico>` è necessario e deve corrispondere all'`ID entità` della configurazione single sign-on. Il valore predefinito è `https://saml.salesforce.com`.

**Destinatario**

Il destinatario specificato in un'asserzione deve corrispondere all'URL di accesso Salesforce specificato nella configurazione di Salesforce o all'endpoint del token OAuth 2.0. Questa è una parte dell'asserzione obbligatoria che viene sempre verificata.

**Firma**

L'asserzione deve contenere una firma valida. La firma deve essere creata utilizzando la chiave privata associata al certificato fornito nella configurazione SAML.

**Destinatario**

Verifica che il destinatario e l'ID organizzazione ricevuti nell'asserzione corrispondano al destinatario e all'ID organizzazione attesi, come specificato nella configurazione Single Sign-On. Questa è una porzione facoltativa dell'asserzione e viene verificata solo se è presente. Ad esempio:

```
Recipient that we found in the assertion: http://aalbert-salesforce.com:8081/
   ?saml=02HKiPoin4zeKLPYxfj3twkPsNSJF3fxsH0Jnq4vVeQr3xNkIWmZC_IVk3
Recipient that we expected based on the Single Sign-On Settings page:
   http://asmith.salesforce.com:8081/
   ?saml=EK03Almz90Cik_ig0L97.0BRme6mT4o6nzi0t_JROL6HLbdR1WVP5aQO5w
Organization Id that we expected: 00Dx0000000BQlI
Organization Id that we found based on your assertion: 00D000000000062
```

**Attributo URL sito**

Verifica se è stato specificato un URL Siti valido. I valori sono:

- Non fornito
- Selezionata
- URL sito non valido
- Per l'URL sito è richiesto HTTPS
- Il sito specificato è inattivo o ha superato il limite di pagina.

VEDERE ANCHE:

Informazioni su SAML

## Informazioni sul provisioning just in time per SAML

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

Con il provisioning just in time è possibile utilizzare un'asserzione SAML per creare utenti normali e utenti portale al momento del loro primo tentativo di accesso. In questo modo non è più necessario creare preventivamente gli account utente. Ad esempio, se un dipendente è stato inserito da poco nella propria organizzazione, non è necessario creare manualmente l'utente in Salesforce. Quando il dipendente effettua l'accesso con il Single Sign-On, l'account viene creato automaticamente senza che sia necessario configurarlo. Il provisioning just in time, in combinazione con il provider di identità SAML, passa i dati corretti dell'utente a Salesforce in un'asserzione SAML 2.0. In questo

modo è possibile creare e modificare gli account. Poiché il provisioning just in time utilizza SAML per la comunicazione, nell'organizzazione deve essere abilitato il Single Sign-On basato su SAML.

## Vantaggi del provisioning just in time

L'implementazione del provisioning just in time può offrire i seguenti vantaggi a un'organizzazione.

- **Riduzione dei costi amministrativi:** il provisioning con SAML consente ai clienti di creare gli account on-demand, durante il processo di Single Sign-On. Questo semplifica notevolmente il lavoro di integrazione necessario nelle situazioni in cui è necessario eseguire il provisioning degli utenti in modo dinamico, combinando le operazioni di provisioning e di Single Sign-On in un unico messaggio.
- **Maggior adozione da parte degli utenti:** per gli utenti è sufficiente memorizzare una sola password per accedere sia al loro sito principale, sia a Salesforce. È quindi più probabile che utilizzino regolarmente l'applicazione Salesforce.
- **Maggior protezione:** gli eventuali criteri per le password in vigore per la rete aziendale saranno applicati anche a Salesforce. Inoltre, l'invio di una credenziale di autenticazione valida per un unico utilizzo può incrementare la sicurezza per gli utenti che hanno accesso a dati sensibili.

VEDERE ANCHE:

Requisiti per il provisioning just in time

Provisioning just in time per i portali

Provisioning just in time per le comunità

Errori di fornitura just in time

Esempi di asserzioni SAML

Informazioni su Single Sign-On

## Requisiti per il provisioning just in time

Il provisioning just in time richiede la creazione di un'asserzione SAML. Quando si crea l'asserzione SAML, prestare attenzione ai seguenti punti.

- `Provision Version` è supportato come attributo facoltativo. Se non è specificato, l'impostazione predefinita è 1.0. Ad esempio:

```
<saml:Attribute Name="ProvisionVersion" NameFormat=
   "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">1.0</saml:AttributeValue>
</saml:Attribute>
```

- Gli ID profilo cambiano a seconda dell'organizzazione, anche per i profili standard. Per facilitare la ricerca del nome di un profilo, Salesforce consente di eseguire una ricerca del nome profilo passando `ProfileName` nel campo `ProfileId`.

### Requisiti dei campi per l'asserzione SAML

Per identificare correttamente l'oggetto da creare in Salesforce è necessario utilizzare il prefisso `User.` per tutti i campi passati nell'asserzione SAML. In questo esempio, il prefisso `User.` è stato aggiunto al nome campo `Username`.

```
<saml:Attribute
   Name="User.Username"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">testuser@123.org</saml:AttributeValue>
</saml:Attribute>
```

Sono supportati i seguenti campi standard.

| Campi | Obbligatorio | Commenti |
| --- | --- | --- |
| AboutMe | | |
| Alias | | Se assente, il valore predefinito viene derivato dai campi FirstName e LastName. |
| CallCenter | | |
| Città | | |
| CommunityNickname | | Se assente, il valore predefinito viene derivato dal campo UserName. |
| CompanyName | | |
| Paese | | |
| DefaultCurrencyIsoCode | | Derivato dalle impostazioni dell'organizzazione. |
| DelegatedApproverId | | |
| Reparto | | |
| Divisione | | |
| Email | Y | Ad esempio, `User.Email=test2@salesforce.com` |
| EmailEncodingKey | | Se assente, il valore predefinito viene derivato dalle impostazioni dell'organizzazione. |
| EmployeeNumber | | |
| Estensione | | |
| Fax | | |
| FederationIdentifier (solo inserimento) | | Se presente, deve corrispondere al subject SAML; in caso contrario, viene utilizzato il subject SAML. Non può essere aggiornato con SAML. |
| FirstName | | |
| ForecastEnabled | | |
| IsActive | | |
| LastName | Y | |
| LanguageLocaleKey | | |
| LocaleSidKey | | Se assente, il valore predefinito viene derivato dalle impostazioni dell'organizzazione. |
| Responsabile | | |
| MobilePhone | | |
| Telefono | | |
| ProfileId | Y | Ad esempio, `User.ProfileId=Standard User` |

| Campi | Obbligatorio | Commenti |
| --- | --- | --- |
| ReceivesAdminInfoEmails | | |
| ReceivesInfoEmails | | |
| Stato | | |
| Via | | |
| TimeZoneSidKey | | Se assente, il valore predefinito viene derivato dalle impostazioni dell'organizzazione. |
| Qualifica | | |
| Username (solo inserimento) | Y | Ad esempio, User.Username=test2@test.com. Non può essere aggiornato mediante SAML. |
| UserRoleId | | Se vuoto, il valore predefinito è "nessun ruolo". |
| CAP | | |

Altri requisiti per i campi:

- Sono supportati solo i campi personalizzati di tipo testo.
- Per i campi personalizzati sono supportate solo le funzioni insert e update.
- Quando si utilizza l'API per la creazione degli utenti è possibile passare il nuovo nome utente nel campo User.Username. È possibile anche specificare il User.FederationIdentifier, se presente. I campi Username e FederationIdentifier non si possono però aggiornare con l'API.

VEDERE ANCHE:

Informazioni sul provisioning just in time per SAML
Provisioning just in time per i portali
Provisioning just in time per le comunità
http://help.salesforce.com/help/pdfs/en/salesforce_communities_implementation.pdf

## Provisioning just in time per i portali

Con il provisioning just in time per i portali è possibile utilizzare un'asserzione SAML per creare utenti portale clienti e partner al momento del loro primo tentativo di accesso. In questo modo non è più necessario creare preventivamente gli account utente. Poiché il provisioning just in time utilizza SAML per la comunicazione, nell'organizzazione deve essere abilitato il Single Sign-On basato su SAML.

**Nota:** a partire dal rilascio Summer '13, i Portali Clienti e i Portali partner non sono più disponibili per le nuove organizzazioni. Le organizzazioni esistenti continuano ad avere accesso a questi portali. Se non si dispone di un portale ma si desidera condividere facilmente le informazioni con i propri clienti o partner, provare a utilizzare le comunità.

Le organizzazioni esistenti che utilizzano i Portali Clienti e i Portali partner possono continuare a utilizzarli o passare alle comunità. Per ulteriori informazioni, rivolgersi al responsabile account Salesforce.

## Creazione di utenti portale

È necessario specificare `ID portale` e `ID organizzazione` come parte dell'asserzione SAML. Entrambi i valori sono indicati nella pagina di informazioni sulla società dell'organizzazione o del portale. Poiché è possibile eseguire il provisioning anche per utenti normali, l'`ID portale` consente di distinguere una richiesta di provisioning just in time normale da una richiesta portale. Se l'`ID portale` non viene specificato, la richiesta viene considerata una richiesta just in time per un utente di piattaforma normale. Di seguito sono elencati i requisiti per la creazione di un utente portale.

- È necessario specificare un `ID federazione`. Se l'ID appartiene a un account utente esistente, l'account utente viene aggiornato. Se l'account utente è inattivo, l'account viene aggiornato ma lasciato inattivo a meno che `User.IsActive` nell'asserzione JIT non sia impostato su vero. Se non sono presenti account utente con l'`ID federazione` specificato, il sistema crea un nuovo utente.
- Se per il portale non è abilitata l'auto registrazione e non sono specificati un nuovo profilo utente e un ruolo predefiniti, il campo `User.ProfileId` deve contenere un nome di profilo o un ID valido associato al portale. Il campo `User.PortalRole` deve inoltre contenere un nome di ruolo portale o un ID valido.

  Nota: `User.Role` deve essere nullo.

## Creazione e modifica degli account

Creare o modificare un account specificando un `ID account` valido oppure i valori `Account.AccountNumber` e `Account.Name`.

- La corrispondenza è basata su `Account.AccountNumber`. In presenza di più account, viene visualizzato un errore. In caso contrario, l'account viene aggiornato.
- Se non viene trovato alcun account corrispondente, viene creato un nuovo account.
- È necessario specificare `Account.Owner` nell'asserzione SAML e assicurarsi che la protezione a livello di campo per il campo `Account.AccountNumber` sia visibile per il profilo del titolare.

## Creazione e modifica dei referenti

Creare o modificare un referente specificando un ID referente valido in `User.Contact` oppure i valori `Contact.Email` e `Contact.LastName`.

- La corrispondenza è basata su `Contact.Email`. In presenza di più referenti, viene visualizzato un errore. In caso contrario, il referente viene aggiornato.
- Se non viene trovato alcun referente corrispondente, viene creato un nuovo referente.

## Campi supportati per l'asserzione SAML del portale

Per identificare correttamente l'oggetto da creare in Salesforce, è necessario usare un prefisso. Nell'asserzione SAML, utilizzare il prefisso `Account` per tutti i campi dello schema Account (ad esempio `Account.AccountId`) e il prefisso `Contact` per tutti i campi dello schema Referente. In questo esempio, il prefisso `Contact` è stato aggiunto al nome campo `Email`.

```
<saml:Attribute
   Name="Contact.Email"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">testuser@123.org</saml:AttributeValue>
</saml:Attribute>
```

In aggiunta ai campi standard supportati per i normali utenti just in time SAML, per gli account sono supportati anche i campi riportati di seguito.

| Campi | Obbligatorio | Commenti |
| --- | --- | --- |
| `Billing` | | Street\|City\|State\|PostalCode\|Country |
| `AnnualRevenue` | | |
| `Description` | | |
| `Fax` | | |
| `FederationIdentifier` (solo inserimento) | Y | Se presente, deve corrispondere al subject SAML; in caso contrario, viene utilizzato il subject SAML. Non può essere aggiornato con SAML. |
| `IsCustomerPortal` | | |
| `IsPartner` | | |
| `NumberOfEmployees` | | |
| `Ownership` | | |
| `Phone` | | |
| `Portal Role` | Y | Utilizzare `Worker` per tutti gli utenti dei portali. |
| `Rating` | | |
| `Street` | | |
| `TickerSymbol` | | |
| `UserRoleId` | | Se vuoto, il valore predefinito è "nessun ruolo". |
| `Website` | | |
| `Zip` | | |

In aggiunta ai campi standard supportati per i normali utenti just in time SAML, per i referenti sono supportati anche i campi riportati di seguito.

| Campi | Obbligatorio | Commenti |
| --- | --- | --- |
| `Birthdate` | | |
| `CanAllowPortalSelfReg` | | Name\|Phone |
| `Department` | | |
| `Description` | | |
| `DoNotCall` | | |
| `Fax` | | |
| `HasOptedOutofEmail` | | |
| `HasOptedOutofFax` | | |
| `HomePhone` | | |

| Campi | Obbligatorio | Commenti |
|---|---|---|
| LeadSource | | |
| Mailing | | Street|City|State|PostalCode|Country |
| MobilePhone | | |
| Owner | | |
| Other | | Street|City|State|PostalCode|Country |
| OtherPhone | | |
| Phone | | |
| Salutation | | |
| Title | | |

VEDERE ANCHE:

Informazioni sul provisioning just in time per SAML

Requisiti per il provisioning just in time

Provisioning just in time per le comunità

http://help.salesforce.com/help/pdfs/en/salesforce_communities_implementation.pdf

## Provisioning just in time per le comunità

Con il provisioning just in time per le comunità è possibile utilizzare un'asserzione SAML per creare utenti delle comunità clienti e partner al momento del loro primo tentativo di accesso da un provider di identità. In questo modo non è più necessario creare preventivamente gli account utente. Poiché il provisioning just in time utilizza SAML per la comunicazione, nell'organizzazione deve essere abilitato il Single Sign-On basato su SAML. In seguito si può collaborare con il provider di identità per generare le asserzioni SAML necessarie per il provisioning just in time.

### Impostazioni Single Sign-On SAML

Seguire le istruzioni per la Configurazione delle impostazioni di SAML per Single Sign-On con `SAML abilitato`. Impostare i valori per la configurazione a seconda delle proprie esigenze e includere anche i seguenti valori specifici della comunità per il provisioning just in time.

1. Selezionare `Provisioning utente abilitato`.

   Nota:

   - Per il provisioning just in time è necessario un ID federazione nel tipo di utente. In `Tipo ID utente SAML`, selezionare L'asserzione contiene l'ID federazione dell'oggetto utente.
   - Se il provider di identità in precedenza utilizzava il nome utente Salesforce, comunicargli che deve utilizzare l'ID federazione.

2. L'**ID entità** deve essere univoco in tutta l'organizzazione e deve iniziare con `https`. Non è possibile avere due configurazioni SAML con lo stesso **ID entità** in una sola organizzazione. Specificare se si desidera utilizzare il dominio di base (`https://saml.salesforce.com`) o l'URL della comunità (ad esempio `https://acme.force.com/customers`) per l'**ID entità**. Questa informazione deve essere condivisa con il provider di identità.

Suggerimento: come regola generale, utilizzare l'URL della comunità come ID entità. Se si forniscono servizi Salesforce a Salesforce è necessario specificare l'URL della comunità.

3. In `Tipo ID utente SAML`, selezionare `L'asserzione contiene l'ID federazione dell'oggetto utente`. Se il provider di identità in precedenza utilizzava il nome utente Salesforce, comunicargli che deve utilizzare l'ID federazione.

## Creazione e modifica di utenti delle comunità

L'asserzione SAML necessita dei seguenti elementi.

- Un URL `Destinatario`, cioè l'URL di accesso alla comunità indicato nella pagina dei dettagli delle Impostazioni Single Sign-On SAML dell'organizzazione. L'URL ha il seguente formato.

  ```
  https://<community_URL>/login?so=<orgID>
  ```

  Ad esempio, `Recipient="https://acme.force.com/customers/login?so=00DD0000000JsCM"` dove `acme.force.com/customers` è la pagina iniziale della comunità e `00DD0000000JsCM` è l'`ID organizzazione`.

  Se nelle Impostazioni Single Sign-On SAML dell'organizzazione è stato caricato un Certificato decrittografia asserzione, includere l'ID del certificato nell'URL mediante il parametro `sc`, ad esempio `Recipient="https://acme.force.com/customers/login?so=00DD0000000JsCM&sc=0LE000000Dp"` dove `0LE000000Dp` è l'ID del certificato.

- Salesforce tenta di trovare una corrispondenza fra l'`ID federazione` nell'oggetto dell'asserzione SAML (o in un elemento Attribute, a seconda di come è definita la Posizione identità SAML nelle Impostazioni Single Sign-On SAML) e il campo `FederationIdentifier` di un record utente esistente.

  1. Se viene trovato un record corrispondente, Salesforce utilizza gli attributi dell'asserzione SAML per aggiornare i campi specificati.
  2. Se non si trova un utente con un record utente corrispondente, Salesforce cerca una corrispondenza fra i referenti con l'`ID account` specificato (`Contact.Account` o `Account.AccountNumber`) e l'ID (`User.ContactId`) o l'email referente (`Contact.Email`).

     i. Se viene trovato un record referente corrispondente, Salesforce utilizza gli attributi dell'asserzione SAML per aggiornare i campi referente specificati, e quindi inserisce un nuovo record utente.

     ii. Se non si trova un record referente corrispondente, Salesforce cerca fra gli account una corrispondenza basata sul `Contact.Account` o sui `Account.AccountNumber` e `Account.Name` specificati nell'asserzione SAML, oppure aggiorna i record referente e utente esistenti dell'account se viene trovata una corrispondenza.

        i. Se viene trovato un record account corrispondente, Salesforce inserisce un nuovo record utente e aggiorna i record account in base agli attributi contenuti nell'asserzione SAML.

        ii. Se non viene trovato un record account corrispondente, Salesforce inserisce un nuovo record account, un nuovo record referente e un nuovo record utente in base agli attributi contenuti nell'asserzione SAML.

  Nel caso di un account utente inattivo, l'account viene aggiornato ma lasciato inattivo a meno che `User.IsActive` nell'asserzione JIT non sia impostato su true. Se non sono presenti account utente con l'`ID federazione` specificato, il sistema crea un nuovo utente.

- Se per la comunità non è abilitata l'auto registrazione e non sono specificati un nuovo profilo utente e un ruolo predefiniti, il campo `User.ProfileId` deve contenere un nome di profilo o un ID valido associato alla comunità.

Salesforce tenta di trovare una corrispondenza fra l'`ID federazione` nell'oggetto dell'asserzione SAML e il campo `FederationIdentifier` di un record utente esistente.

Nota: nell'asserzione SAML, Salesforce supporta anche i campi personalizzati sull'oggetto Utente. Tutti gli attributi dell'asserzione che iniziano con `User` vengono analizzati come campi personalizzati. Ad esempio, l'attributo

User.NumberOfProductsBought__c nell'asserzione viene collocato nel campo NumberOfProductsBought per l'utente con provisioning. I campi personalizzati non sono supportati per Account e Referenti.

## Campi supportati per l'asserzione SAML della comunità

Per identificare correttamente l'oggetto da creare in Salesforce, è necessario usare un prefisso. Nell'asserzione SAML, utilizzare il prefisso Account per tutti i campi dello schema Account (ad esempio Account.AccountId) e il prefisso Contact per tutti i campi dello schema Referente. In questo esempio, il prefisso Contact è stato aggiunto al nome campo Email.

```
<saml:Attribute
   Name="Contact.Email"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:anyType">testuser@123.org</saml:AttributeValue>
</saml:Attribute>
```

In aggiunta ai campi standard supportati per i normali utenti just in time SAML, per gli account sono supportati anche i campi riportati di seguito.

| Campi | Obbligatorio | Commenti |
|---|---|---|
| Billing | | Street\|City\|State\|PostalCode\|Country |
| AnnualRevenue | | |
| Descrizione | | |
| Fax | | |
| FederationIdentifier (solo inserimento) | Y | Se presente, deve corrispondere al subject SAML; in caso contrario, viene utilizzato il subject SAML. Non può essere aggiornato con SAML. |
| IsCustomerPortal | | |
| IsPartner | | |
| NumberOfEmployees | | |
| Proprietà | | |
| Telefono | | |
| Portal Role | | |
| Valutazione | | |
| Via | | |
| TickerSymbol | | |
| UserRoleId | | Se vuoto, il valore predefinito è "nessun ruolo". |
| Sito Web | | |
| CAP | | |

In aggiunta ai campi standard supportati per i normali utenti just in time SAML, per i referenti sono supportati anche i campi riportati di seguito.

| Campi | Obbligatorio | Commenti |
| --- | --- | --- |
| `Compleanno` | | |
| `CanAllowPortalSelfReg` | | Name\|Phone |
| `Reparto` | | |
| `Descrizione` | | |
| `DoNotCall` | | |
| `Fax` | | |
| `HasOptedOutofEmail` | | |
| `HasOptedOutofFax` | | |
| `HomePhone` | | |
| `LeadSource` | | |
| `Mailing` | | Street\|City\|State\|PostalCode\|Country |
| `MobilePhone` | | |
| `Titolare` | | |
| `Other` | | Street\|City\|State\|PostalCode\|Country |
| `OtherPhone` | | |
| `Telefono` | | |
| `Titolo` | | |
| `Qualifica` | | |

VEDERE ANCHE:

Informazioni sul provisioning just in time per SAML

Requisiti per il provisioning just in time

http://help.salesforce.com/help/pdfs/en/salesforce_communities_implementation.pdf

## Errori di fornitura just in time

Di seguito sono riportati i codici di errore relativi alla fornitura just in time per SAML e le relative descrizioni.

Gli errori SAML vengono restituiti nel parametro dell'URL, ad esempio:

```
http://login.salesforce.com/identity/jit/saml-error.jsp?
ErrorCode=5&ErrorDescription=Unable+to+create+user&ErrorDetails=
INVALID_OR_NULL_FOR_RESTRICTED_PICKLIST+TimeZoneSidKey
```

**Nota:** Salesforce reindirizza l'utente a un URL di errore personalizzato se questo viene specificato nella configurazione SAML.

## Messaggi di errore

| Codice | Descrizione | Dettagli errore |
|---|---|---|
| 1 | ID federazione mancante | MISSING_FEDERATION_ID |
| 2 | Mancata corrispondenza ID federazione | MISMATCH_FEDERATION_ID |
| 3 | ID organizzazione non valido | INVALID_ORG_ID |
| 4 | Impossibile acquisire il blocco | USER_CREATION_FAILED_ON_UROG |
| 5 | Impossibile creare l'utente | USER_CREATION_API_ERROR |
| 6 | Impossibile stabilire il contesto amministratore | ADMIN_CONTEXT_NOT_ESTABLISHED |
| 8 | Campo personalizzato non riconosciuto | UNRECOGNIZED_CUSTOM_FIELD |
| 9 | Campo standard non riconosciuto | UNRECOGNIZED_STANDARD_FIELD |
| 11 | Limite licenza superato | LICENSE_LIMIT_EXCEEDED |
| 12 | Mancata corrispondenza tra ID federazione e nome utente | MISMATCH_FEDERATION_ID_AND_USERNAME_ATTRS |
| 13 | Versione API fornitura non supportata | UNSUPPORTED_VERSION |
| 14 | Modifica del nome utente non consentita | USER_NAME_CHANGE_NOT_ALLOWED |
| 15 | Tipo di campo personalizzato non supportato | UNSUPPORTED_CUSTOM_FIELD_TYPE |
| 16 | Impossibile mappare un ID profilo univoco per il nome profilo fornito | PROFILE_NAME_LOOKUP_ERROR |
| 17 | Impossibile mappare un ID ruolo univoco per il nome ruolo fornito | ROLE_NAME_LOOKUP_ERROR |
| 18 | Account non valido | INVALID_ACCOUNT_ID |
| 19 | Nome account mancante | MISSING_ACCOUNT_NAME |
| 20 | Numero account mancante | MISSING_ACCOUNT_NUMBER |
| 22 | Impossibile creare l'account | ACCOUNT_CREATION_API_ERROR |
| 23 | Referente non valido | INVALID_CONTACT |
| 24 | Email referente mancante | MISSING_CONTACT_EMAIL |
| 25 | Cognome referente mancante | MISSING_CONTACT_LAST_NAME |
| 26 | Impossibile creare il referente | CONTACT_CREATION_API_ERROR |
| 27 | Trovati più referenti corrispondenti | MULTIPLE_CONTACTS_FOUND |
| 28 | Trovati più account corrispondenti | MULTIPLE_ACCOUNTS_FOUND |
| 30 | Titolare account non valido | INVALID_ACCOUNT_OWNER |
| 31 | Profilo portale non valido | INVALID_PORTAL_PROFILE |

| Codice | Descrizione | Dettagli errore |
|---|---|---|
| 32 | Cambio account non consentito | ACCOUNT_CHANGE_NOT_ALLOWED |
| 33 | Impossibile aggiornare l'account | ACCOUNT_UPDATE_FAILED |
| 34 | Impossibile aggiornare il referente | CONTACT_UPDATE_FAILED |
| 35 | Valore campo account standard non valido | INVALID_STANDARD_ACCOUNT_FIELD_VALUE |
| 36 | Cambio referente non consentito | CONTACT_CHANGE_NOT_ALLOWED |
| 37 | Ruolo portale non valido | INVALID_PORTAL_ROLE |
| 38 | Impossibile aggiornare il ruolo portale | CANNOT_UPDATE_PORTAL_ROLE |
| 39 | Classe handler JIT SAML non valida | INVALID_JIT_HANDLER |
| 40 | Utente esecuzione non valido | INVALID_EXECUTION_USER |
| 41 | Errore di esecuzione | APEX_EXECUTION_ERROR |
| 42 | L'aggiornamento di un referente con account personale non è supportato | UNSUPPORTED_CONTACT_PERSONACCT_UPDATE |

VEDERE ANCHE:

Informazioni sul provisioning just in time per SAML

Provisioning just in time per i portali

# Informazioni sui provider di autenticazione esterni

È possibile abilitare gli utenti in modo che possano accedere alla propria organizzazione Salesforce utilizzando le loro credenziali di accesso di un provider di servizi esterno, quale Facebook© o Janrain©.

Per impostare correttamente un provider di autenticazione per il Single Sign-On, attenersi alla seguente procedura.

- Configurare correttamente il sito Web del provider di servizio.
- Creare un handler registrazione utilizzando Apex.
- Definire il provider di autenticazione nella poropria organizzazione.

Una volta completata l'impostazione, il flusso del provider di autenticazione è il seguente.

1. L'utente tenta di accedere a Salesforce utilizzando un'identità di terze parti.
2. La richiesta di accesso viene reindirizzata al provider di autenticazione di terze parti.
3. L'utente segue il procedimento di accesso di terze parti e approva l'accesso.
4. Il provider di autenticazione di terze parti reindirizza l'utente a Salesforce con le credenziali.
5. L'accesso dell'utente a Salesforce è stato eseguito.

Nota: Se l'utente dispone di una sessione di Salesforce esistente, dopo l'autenticazione di terze parti, viene automaticamente reindirizzato alla pagina nella quale può approvare il link al proprio account Salesforce.

EDIZIONI

Disponibile nelle versioni: Lightning Experience e Salesforce Classic

Disponibile in: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:
- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:
- "Personalizza applicazione"

  E

  "Gestisci provider di autenticazione"

## Definizione del provider di autenticazione

Sono supportati i seguenti provider:

- Facebook
- Google
- Janrain
- LinkedIn
- Microsoft Access Control Service
- Salesforce
- Twitter
- Qualsiasi provider di servizi che implementi il protocollo OpenID Connect

## Aggiunta di funzionalità al provider di autenticazione

È possibile aggiungere funzionalità al provider di autenticazione utilizzando parametri di richiesta aggiuntivi.

- Scope – Personalizza le autorizzazioni richieste da terze parti
- Site – Consente di utilizzare il provider con un sito
- StartURL – Invia l'utente a un indirizzo specifico dopo l'autenticazione
- Community – Indirizza l'utente a una comunità specifica dopo l'autenticazione
- Authorization Endpoint a pagina 628 – Invia l'utente a un endpoint specifico per l'autenticazione (solo provider di autenticazione Salesforce)

## Creazione di un handler registrazione Apex

È necessaria una classe handler di registrazione per utilizzare Provider di autenticazione per il flusso Single Sign-On. La classe handler di registrazione Apex deve implementare l'interfaccia `Auth.RegistrationHandler`, che definisce due metodi. Salesforce invoca il metodo appropriato sulla richiamata a seconda che l'utente abbia utilizzato questo provider in passato oppure no. Quando si crea il provider di autenticazione, è possibile creare automaticamente una classe di modelli Apex per scopi di test.

## Configurazione di un provider di autenticazione Facebook

EDIZIONI

Disponibile nelle versioni: Lightning Experience e Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:
- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:
- "Personalizza applicazione"

  E

  "Gestisci provider di autenticazione"

Per utilizzare Facebook come provider di autenticazione:

1. Impostare un'applicazione Facebook con Salesforce come dominio dell'applicazione.
2. Definire il provider di autenticazione Facebook nell'organizzazione Salesforce.
3. Aggiornare l'applicazione Facebook in modo che utilizzi l'`URL di richiamata` generato da Salesforce come `URL sito Web` di Facebook.
4. Provare la connessione.

### Impostazione di un'applicazione Facebook

Per poter configurare Facebook per l'organizzazione Salesforce, è necessario prima impostare un'applicazione in Facebook:

Nota: questo passaggio si può saltare consentendo a Salesforce di usare l'applicazione predefinita. Per ulteriori informazioni, vedere Uso dei valori gestiti da Salesforce nell'impostazione dei provider di autenticazione.

1. Accedere al sito Web Facebook e creare una nuova applicazione.
2. Modificare le impostazioni dell'applicazione e impostare il dominio dell'applicazione su Salesforce.
3. Annotare l'ID e il segreto dell'applicazione.

### Definizione di un provider Facebook nell'organizzazione Salesforce

Per impostare un provider Facebook nell'organizzazione Salesforce, è necessario disporre dell'ID e del segreto dell'applicazione.

Nota: è possibile evitare di specificare questi valori chiave nell'impostazione del provider affidando a Salesforce la gestione dei valori. Per ulteriori informazioni, vedere Uso dei valori gestiti da Salesforce nell'impostazione dei provider di autenticazione.

1. Da Imposta, immettere *`Provider di autenticazione`* nella casella `Ricerca veloce`, quindi selezionare **Provider di autenticazione**.
2. Fare clic su **Nuovo**.
3. Selezionare Facebook per `Tipo provider`.
4. Immettere un `Nome` per il provider.
5. Immettere il `Suffisso URL`, Viene utilizzato negli URL di configurazione client. Ad esempio, se il suffisso URL del provider è "MyFacebookProvider", l'URL Single Sign-On è simile a: `https://login.salesforce.com/auth/sso/00Dx00000000001/MyFacebookProvider`.
6. Utilizzare l'ID dell'applicazione di Facebook per il campo `Chiave consumatore`.

7. Utilizzare il segreto dell'applicazione di Facebook per il campo `Segreto consumatore`.
8. Se lo si desidera, impostare i campi che seguono.
   a. Immettere l'URL di base di Facebook per il campo `Autorizza URL endpoint`. Ad esempio, `https://www.facebook.com/v2.2/dialog/oauth`. Se si lascia vuoto il campo, Salesforce utilizza la versione dell'API Facebook utilizzata dall'applicazione.

      Suggerimento: se necessario è possibile aggiungere all'URL di base dei parametri della stringa di query. Ad esempio, per ottenere un token di aggiornamento da Google per l'accesso offline, utilizzare `https://accounts.google.com/o/oauth2/auth?access_type=offline&approval_prompt=force`. In questo esempio, il parametro `approval_prompt` aggiuntivo è necessario per chiedere all'utente di accettare l'azione di aggiornamento, in modo che Google continui a fornire token di aggiornamento dopo il primo token.

   b. Immettere l'`URL endpoint token` di Facebook. Ad esempio, `https://www.facebook.com/v2.2/dialog/oauth`. Se si lascia vuoto il campo, Salesforce utilizza la versione dell'API Facebook utilizzata dall'applicazione.
   c. Immettere l'`URL endpoint info utente` per modificare i valori richiesti dall'API del profilo Facebook. Per ulteriori informazioni sui campi, vedere https://developers.facebook.com/docs/facebook-login/permissions/v2.0#reference-public_profile. I campi richiesti devono corrispondere agli ambiti richiesti. Se si lascia vuoto il campo, Salesforce utilizza la versione dell'API Facebook utilizzata dall'applicazione.
   d. `Ambiti predefiniti` da inviare insieme alla richiesta all'endpoint di autorizzazione. In caso contrario vengono utilizzate le impostazioni predefinite codificate per il tipo di provider (per l'elenco delle impostazioni predefinite, vedere la documentazione per sviluppatori Facebook).

      Per ulteriori informazioni, vedere Uso del parametro Scope.

   e. `URL di errore personalizzato` utilizzato dal provider per segnalare eventuali errori.
   f. `URL di disconnessione personalizzato` per fornire una destinazione specifica agli utenti autenticati con il flusso Single Sign-On che si disconnettono. Usare questo campo per indirizzare gli utenti a una pagina di disconnessione con l'immagine aziendale o a una destinazione diversa dalla pagina di disconnessione predefinita di Salesforce. L'URL deve essere completo e dotato di prefisso `http` o `https`, ad esempio `https://acme.my.salesforce.com`.
   g. Selezionare una classe Apex già esistente come classe `Handler registrazione` o fare clic su `Crea automaticamente un modello di handler registrazione` per creare un modello di classe Apex per l'handler di registrazione. È necessario modificare questa classe e il contenuto predefinito prima di utilizzarlo.

      Nota: per consentire a Salesforce di generare l'`URL inizializzazione Single Sign-On`, è necessario specificare una classe di handler registrazione.

   h. Selezionare l'utente che esegue la classe di handler Apex per **Esegui registrazione come**. L'utente deve disporre dell'autorizzazione "Gestisci utenti". È richiesto un utente se è stata selezionata una classe di handler registrazione o se se ne sta creando automaticamente una.
   i. Per utilizzare un portale con il provider, selezionare il portale dall'elenco a discesa Portale.
   j. Utilizzare il campo `URL icona` per associare un percorso a un'icona da visualizzare come pulsante nella pagina di accesso di una comunità. L'icona è valida solo per una comunità, e non compare nella pagina di accesso dell'organizzazione Salesforce o nel dominio personalizzato creato con Dominio personale. Gli utenti fanno clic sul pulsante per accedere con il provider di autenticazione associato della comunità.

      È possibile specificare il percorso di un'immagine personalizzata, oppure copiare nel campo l'URL di una delle icone di esempio.

9. Fare clic su **Salva**.

Assicurarsi di annotare il valore `ID provider di autenticazione` generato. È necessario utilizzarlo con la classe Apex `Auth.AuthToken`.

Dopo la definizione del provider di autenticazione vengono generati alcuni URL di configurazione client:

- `URL inizializzazione solo test`: gli amministratori utilizzano questo URL per assicurarsi che il provider di terze parti sia impostato correttamente. L'amministratore apre l'URL in un browser, accede al provider di terze parti e viene di nuovo reindirizzato a Salesforce con una mappa di attributi.
- `URL inizializzazione Single Sign-On`: utilizzare questo URL per eseguire il Single Sign-On in Salesforce da un provider di terze parti (con credenziali di terze parti). L'utente finale apre questo URL in un browser e accede al provider di terze parti. Successivamente crea un nuovo utente oppure aggiorna un utente già esistente, quindi effettua l'accesso a Salesforce come tale utente.
- `URL di collegamento utente esistente`: utilizzare questo URL per collegare gli utenti Salesforce esistenti a un account di terze parti. L'utente finale apre questo URL in un browser, accede al provider di terze parti, accede a Salesforce e approva il link.
- `URL inizializzazione solo Oauth`: Utilizzare questo URL per ottenere token di accesso OAuth per una terza parte. Affinché il servizio di terzi ottenga il token, gli utenti devono eseguire l'autenticazione in Salesforce; questo flusso non è predisposto per una futura funzionalità di Single Sign-On.
- `URL di richiamata`: utilizzare l'URL di richiamata per l'endpoint che il provider di autenticazione richiama per la configurazione. Il provider di autenticazione deve reindirizzare all'`URL di richiamata` con le informazioni per ciascuno degli URL di configurazione client di cui sopra.

Gli URL di configurazione client supportano ulteriori parametri di richiesta che consentono di richiedere agli utenti di accedere a specifici siti, ottenere autorizzazioni personalizzate da terze parti o passare a un percorso specifico dopo l'autenticazione.

### Aggiornamento dell'applicazione Facebook

Dopo aver definito il provider di autenticazione Facebook nell'organizzazione Salesforce, tornare a Facebook e aggiornare l'applicazione in modo che utilizzi l'`URL di richiamata` come `URL sito Web` di Facebook.

### Test della connessione Single Sign-On

In un browser, aprire l'`URL inizializzazione solo test` nella pagina dei dettagli del provider di autenticazione. Dovrebbe reindirizzare a Facebook e chiedere di effettuare l'accesso. Una volta effettuato l'accesso, viene richiesta l'autorizzazione dell'applicazione. Dopo avere concesso l'autorizzazione si è nuovamente indirizzati a Salesforce.

VEDERE ANCHE:

Uso dei parametri di richiesta con URL di configurazione client

Informazioni sui provider di autenticazione esterni

## Configurazione di un provider di autenticazione Google

Consente agli utenti di accedere a un'organizzazione Salesforce con i loro account Google.

Per utilizzare Google come provider di autenticazione:

1. Impostare un'applicazione Google con Salesforce come dominio dell'applicazione.
2. Definire un provider di autenticazione Google nell'organizzazione Salesforce.
3. Aggiornare l'applicazione Google in modo che utilizzi l'`URL di richiamata` generato da Salesforce come `URL sito Web` di Google.
4. Provare la connessione.

EDIZIONI

Disponibile nelle versioni: Lightning Experience e Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:
- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:
- "Personalizza applicazione"

  E

  "Gestisci provider di autenticazione"

### Impostare un'applicazione Google

Per poter configurare Google per l'organizzazione Salesforce, è necessario prima impostare un'applicazione in Google:

Nota: questo passaggio si può saltare consentendo a Salesforce di usare l'applicazione predefinita. Per ulteriori informazioni, vedere Uso dei valori gestiti da Salesforce nell'impostazione dei provider di autenticazione.

1. Accedere al sito Web Google e creare una nuova applicazione.
2. Modificare le impostazioni dell'applicazione e impostare il dominio dell'applicazione su Salesforce.
3. Annotare l'ID e il segreto dell'applicazione.

### Definire un provider Google nell'organizzazione Salesforce

Per impostare un provider Google nell'organizzazione Salesforce, è necessario disporre dell'ID e del segreto dell'applicazione.

Nota: è possibile evitare di specificare questi valori chiave nell'impostazione del provider affidando a Salesforce la gestione dei valori. Per ulteriori informazioni, vedere Uso dei valori gestiti da Salesforce nell'impostazione dei provider di autenticazione.

1. Da Imposta, immettere *`Provider di autenticazione`* nella casella `Ricerca veloce`, quindi selezionare **Provider di autenticazione**.
2. Fare clic su **Nuovo**.
3. Selezionare Google per `Tipo provider`.
4. Immettere un `Nome` per il provider.
5. Immettere il `Suffisso URL` utilizzato negli URL della configurazione client. Ad esempio, se il suffisso URL del provider è "MyGoogleProvider", l'URL Single Sign-On è simile a: `https://login.salesforce.com/auth/sso/00Dx00000000001/MyGoogleProvider`.
6. Utilizzare l'ID dell'applicazione di Google per il campo `Chiave consumatore`.
7. Utilizzare il segreto dell'applicazione di Google per il campo `Segreto consumatore`.
8. Se lo si desidera, impostare i campi che seguono.
   a. `Autorizza URL endpoint` per specificare l'URL di autorizzazione di base da Google. Ad esempio, `https://accounts.google.com/o/oauth2/authorize`. L'URL deve iniziare con *`https://accounts.google.com/o/oauth2`*.

Suggerimento: Se necessario è possibile aggiungere all'URL di base dei parametri della stringa di query. Ad esempio, per ottenere un token di aggiornamento da Google per l'accesso offline, utilizzare `https://accounts.google.com/o/oauth2/auth?access_type=offline&approval_prompt=force`. Il parametro `approval_prompt` è necessario per chiedere all'utente di accettare l'azione di aggiornamento, in modo che Google continui a fornire token di aggiornamento dopo il primo token.

b. `Url endpoint token` per specificare l'URL token OAuth da Google. Ad esempio, `https://accounts.google.com/o/oauth2/accessToken`. L'URL deve iniziare con *`https://accounts.google.com/o/oauth2`*.

c. `URL endpoint info utente` per modificare i valori richiesti dall'API del profilo Google. L'URL deve iniziare con *`https://www.googleapis.com/oauth2/`*.

d. `Ambiti predefiniti` da inviare insieme alla richiesta all'endpoint di autorizzazione. In caso contrario vengono utilizzate le impostazioni predefinite codificate per il tipo di provider. Per i valori predefiniti, vedere la documentazione per sviluppatori Google.

   Per ulteriori informazioni, vedere Uso del parametro Scope.

e. `URL di errore personalizzato` per specificare l'URL che il provider può utilizzare per segnalare eventuali errori.

f. `URL di disconnessione personalizzato` per fornire una destinazione specifica agli utenti autenticati con il flusso Single Sign-On che si disconnettono. Usare questo campo per indirizzare gli utenti a una pagina di disconnessione con l'immagine aziendale o a una destinazione diversa dalla pagina di disconnessione predefinita di Salesforce. L'URL deve essere completo e dotato di prefisso `http` o `https`, ad esempio `https://acme.my.salesforce.com`.

g. Per creare un modello di classe Apex per l'handler di registrazione, selezionare una classe Apex esistente come classe `Handler registrazione` o fare clic su `Crea automaticamente un modello di handler registrazione`. Modificare questa classe e modificare il contenuto predefinito prima di utilizzarlo.

   Nota: specificare una classe di handler registrazione per consentire a Salesforce di generare l'`URL inizializzazione Single Sign-On`.

h. Selezionare l'utente che esegue la classe di handler Apex per **Esegui registrazione come**. L'utente deve disporre dell'autorizzazione "Gestisci utenti". È necessario specificare un utente se è stata selezionata una classe di handler registrazione o se se ne sta creando automaticamente una.

i. Per utilizzare un portale con il provider, selezionare il portale dall'elenco `Portale`.

j. Utilizzare il campo `URL icona` per associare un percorso a un'icona da visualizzare come pulsante nella pagina di accesso di una comunità. L'icona è valida solo per una comunità, e non compare nella pagina di accesso dell'organizzazione Salesforce o nel dominio personalizzato creato con Dominio personale. Gli utenti fanno clic sul pulsante per accedere con il provider di autenticazione associato della comunità.

   È possibile specificare il percorso di un'immagine personalizzata, oppure copiare nel campo l'URL di una delle icone di esempio.

9. Fare clic su **Salva**.

Prendere nota del valore `ID provider di autenticazione` generato. Il valore viene utilizzato con la classe Apex `Auth.AuthToken`.

Dopo la definizione del provider di autenticazione vengono generati alcuni URL di configurazione client:

- `URL inizializzazione solo test`: gli amministratori utilizzano questo URL per assicurarsi che il provider di terze parti sia impostato correttamente. L'amministratore apre l'URL in un browser, accede al provider di terze parti e viene di nuovo reindirizzato a Salesforce con una mappa di attributi.

- `URL inizializzazione Single Sign-On`: utilizzare questo URL per eseguire il Single Sign-On in Salesforce da un provider di terze parti (con credenziali di terze parti). L'utente finale apre questo URL in un browser e accede al provider di terze parti. Questi crea un utente oppure aggiorna un utente già esistente, quindi effettua l'accesso a Salesforce come tale utente.
- `URL di collegamento utente esistente`: utilizzare questo URL per collegare gli utenti Salesforce esistenti a un account di terze parti. L'utente finale apre questo URL in un browser, accede al provider di terze parti, accede a Salesforce e approva il link.
- `URL inizializzazione solo Oauth`: Utilizzare questo URL per ottenere token di accesso OAuth per una terza parte. Affinché il servizio di terzi ottenga il token, gli utenti devono eseguire l'autenticazione in Salesforce; questo flusso non è predisposto per una futura funzionalità di Single Sign-On.
- `URL di richiamata`: utilizzare l'URL di richiamata per l'endpoint che il provider di autenticazione richiama per la configurazione. Il provider di autenticazione reindirizza all'`URL di richiamata` con le informazioni per ciascuno degli URL di configurazione client.

Gli URL di configurazione client supportano ulteriori parametri di richiesta che consentono di richiedere agli utenti di accedere a specifici siti, ottenere autorizzazioni personalizzate da terze parti o passare a un percorso dopo l'autenticazione.

## Aggiornare l'applicazione Google

Dopo aver definito il provider di autenticazione Google nell'organizzazione Salesforce, tornare a Google e aggiornare l'applicazione in modo che utilizzi l'`URL di richiamata` come `URL sito Web` di Google.

## Provare la connessione Single Sign-On

In un browser, aprire l'`URL inizializzazione solo test` nella pagina dei dettagli del provider di autenticazione. Reindirizza a Google e chiede di eseguire l'accesso. Viene quindi richiesta l'autorizzazione dell'applicazione. Dopo avere concesso l'autorizzazione si è nuovamente indirizzati a Salesforce.

## Configurazione di un provider di autenticazione Janrain

L'impostazione di un provider di autenticazione Janrain è leggermente diversa da quella di altri provider. Per avviare il flusso non si utilizza l'URL di inizializzazione Single Sign-On che si ottiene dopo la registrazione del provider con Salesforce. Si utilizza invece il widget di accesso di Janrain distribuito sul sito.

Per impostare il provider Janrain:

1. Registrare l'applicazione su Janrain e ottenere un `apiKey`.
2. Definire il provider di autenticazione Janrain nell'organizzazione Salesforce.
3. Ottenere il codice del widget di accesso da Janrain.
4. Impostare un sito che richiami il codice del widget di accesso nell'organizzazione Salesforce.

EDIZIONI

Disponibile nelle versioni: Lightning Experience e Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:
- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:
- "Personalizza applicazione"

  E

  "Gestisci provider di autenticazione"

### Registrazione dell'applicazione

È necessario creare un account Janrain sul sito Web Janrain. Quando si dispone dell'account Janrain, è necessario un `apiKey`.

1. Fare clic su **Deployment** > **Sign-in for Web** > **Handle Tokens**.
2. Copiare l'`apiKey` che sarà necessario per la creazione del provider Janrain nell'organizzazione Salesforce.
3. Aggiungere `Salesforce` alla whitelist dei domini Janrain nel proprio account Janrain in **Deployment** > **Application Settings** > **Domain Whitelist**.

### Definizione del provider Janrain nell'organizzazione Salesforce

Per creare un provider Janrain nella propria organizzazione Salesforce è necessario disporre dell'`apiKey` Janrain.

1. Da Imposta, immettere *`Provider di autenticazione`* nella casella `Ricerca veloce`, quindi selezionare **Provider di autenticazione**.
2. Fare clic su **Nuovo**.
3. Selezionare Janrain per `Tipo provider`.
4. Immettere un `Nome` per il provider.
5. Immettere il `Suffisso URL`. Viene utilizzato nell'`URL di richiamata`. Ad esempio, se il suffisso dell'URL del provider è "MyJanrainProvider", l'`URL di richiamata` è simile a `https://login.salesforce.com/services/authcallback/00D300000007CvvEAE/MyJanrainProvider`.
6. Utilizzare il valore `apiKey` di Janrain per il `Segreto consumatore`.
7. Se necessario, immettere un `URL di errore personalizzato` che il provider può utilizzare per segnalare eventuali errori.
8. Se necessario, immettere un `URL di disconnessione personalizzato` per fornire una destinazione specifica agli utenti autenticati con il flusso Single Sign-On che si disconnettono. Usare questo campo per indirizzare gli utenti a una pagina di disconnessione con l'immagine aziendale o a una destinazione diversa dalla pagina di disconnessione predefinita di Salesforce. L'URL deve essere completo e dotato di prefisso `http` o `https`, ad esempio `https://acme.my.salesforce.com`.
9. Selezionare una classe Apex già esistente, ad esempio la classe `Handler registrazione`, o fare clic su `Crea automaticamente un modello di handler registrazione` per creare il modello di classe Apex per l'handler di registrazione. È necessario modificare questa classe per modificare il contenuto predefinito prima di utilizzarlo.

Nota: Specificare una classe di handler registrazione per Salesforce per l'uso del Single Sign-On.

10. Selezionare l'utente che esegue la classe di handler Apex per **Esegui registrazione come**. L'utente deve disporre dell'autorizzazione "Gestisci utenti". È richiesto un utente se è stata selezionata una classe di handler registrazione o se se ne sta creando automaticamente una.
11. Per utilizzare un portale con il provider, selezionare il portale dall'elenco a discesa Portale.
12. Utilizzare il campo `URL icona` per associare un percorso a un'icona da visualizzare come pulsante nella pagina di accesso di una comunità. L'icona è valida solo per una comunità, e non compare nella pagina di accesso dell'organizzazione Salesforce o nel dominio personalizzato creato con Dominio personale. Gli utenti fanno clic sul pulsante per accedere con il provider di autenticazione associato della comunità.

    È possibile specificare il percorso di un'immagine personalizzata, oppure copiare nel campo l'URL di una delle icone di esempio.

13. Fare clic su **Salva**.

Prendere nota del valore dell'`URL di richiamata` generato. che sarà necessario per completare l'impostazione di Janrain.

Sono disponibili diversi parametri di configurazione client dopo aver configurato Janrain come provider di autenticazione. Utilizzarli per il valore `flowtype` nell'`URL di richiamata` con il widget di accesso Janrain:

- `test`: utilizzare questo parametro per assicurarsi che il provider di terze parti sia impostato correttamente. L'amministratore configura un widget Janrain per utilizzare `flowtype=test`, esegue l'accesso al provider di terze parti e viene di nuovo reindirizzato a Salesforce con una mappa di attributi.
- `link`: utilizzare questo parametro per collegare gli utenti Salesforce esistenti a un account di terze parti. L'utente finale accede a una pagina con un widget Janrain configurato per l'uso di `flowtype=link`, accede al provider di terze parti, accede a Salesforce e approva il link.
- `sso`: utilizzare questo parametro per eseguire il Single Sign-On a Salesforce da un provider di terze parti (con credenziali di terze parti). L'utente finale accede a una pagina con un widget Janrain configurato per l'uso di `flowtype=sso` e accede al provider di terze parti. Successivamente crea un nuovo utente oppure aggiorna un utente già esistente, quindi effettua l'accesso a Salesforce come tale utente.

Gli URL di configurazione client supportano ulteriori parametri di richiesta che consentono di richiedere agli utenti di accedere a specifici siti, ottenere autorizzazioni personalizzate da terze parti o passare a un percorso specifico dopo l'autenticazione.

## Richiesta del codice del widget di accesso a Janrain

È necessario richiedere a Janrain il codice del widget di accesso per l'organizzazione Salesforce.

1. Dall'account Janrain, fare clic su **Application** > **Sign-in for Web** > **Get the Code**.
2. Immettere il valore dell'`URL di richiamata` fornito dal provider Janrain nella propria organizzazione Salesforce insieme al parametro di query *`flowtype=sso`* come URL del token. Ad esempio

    ```
    https://login.salesforce.com/services/authcallback/00DD##############/JanrainApp?flowtype=sso
    ```

    Per un dominio personalizzato creato con Dominio personale, sostituire a `login.salesforce.com` il nome di Dominio personale.

    Per una comunità, aggiungere il parametro `community` e trasmetterlo al widget di accesso come URL token. Ad esempio

    ```
    janrain.settings.tokenUrl='https://login.salesforce.com/services/authcallback/00DD##############/JanrainApp'
    +'?flowtype=sso&community='+encodeURIComponent('https://acme.force.com/customers');
    ```

### Creazione di un sito per chiamare il widget di accesso

1. Abilitare Sites.
2. Creare una pagina e copiare il codice del widget di accesso nella pagina.
3. Creare un nuovo sito e specificare la pagina appena creata come pagina iniziale per il sito.

VEDERE ANCHE:

Uso dei parametri di richiesta con URL di configurazione client

Informazioni sui provider di autenticazione esterni

http://help.salesforce.com/help/pdfs/en/salesforce_communities_implementation.pdf

## Configurazione di un provider di autenticazione Salesforce

EDIZIONI

Disponibile nelle versioni: Lightning Experience e Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:

- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:

- "Personalizza applicazione"

  E

  "Gestisci provider di autenticazione"

È possibile utilizzare un'applicazione connessa come provider di autenticazione. Eseguire le operazioni indicate di seguito:

1. Definire un'applicazione connessa
2. Definire il provider di autenticazione Salesforce nell'organizzazione.
3. Provare la connessione.

### Definire un'applicazione connessa

Per configurare un provider Salesforce per l'organizzazione Salesforce, è necessario definire un'applicazione connessa che utilizzi il Single Sign-On. Da Imposta, immettere *`Applicazioni`* nella casella `Ricerca veloce`, quindi selezionare **Applicazioni**.

Dopo avere completato la definizione dell'applicazione connessa, salvare i valori dei campi `Chiave consumatore` e `Segreto consumatore`.

Nota: questo passaggio si può saltare consentendo a Salesforce di usare l'applicazione predefinita. Per ulteriori informazioni, vedere Uso dei valori gestiti da Salesforce nell'impostazione dei provider di autenticazione.

### Definire il provider di autenticazione Salesforce nell'organizzazione

Per impostare il provider di autenticazione nella propria organizzazione, sono necessari i valori dei campi `Chiave consumatore` e `Segreto consumatore` della definizione dell'applicazione connessa.

Nota: è possibile evitare di specificare questi valori chiave nell'impostazione del provider affidando a Salesforce la gestione dei valori. Per ulteriori informazioni, vedere Uso dei valori gestiti da Salesforce nell'impostazione dei provider di autenticazione.

1. Da Imposta, immettere *`Provider di autenticazione`* nella casella `Ricerca veloce`, quindi selezionare **Provider di autenticazione**.
2. Fare clic su **Nuovo**.
3. Selezionare Salesforce per `Tipo provider`.
4. Immettere un `Nome` per il provider.

5. Immettere il `Suffisso URL`. Viene utilizzato negli URL di configurazione client. Ad esempio, se il suffisso URL del provider è "MySFDCProvider", l'URL Single Sign-On è simile a `https://login.salesforce.com/auth/sso/00Dx00000000001/MySFDCProvider`.
6. Incollare il valore di `Chiave consumatore` della definizione dell'applicazione connessa nel campo `Chiave consumatore`.
7. Incollare il valore di `Segreto consumatore` della definizione dell'applicazione connessa nel campo `Segreto consumatore`.
8. Se lo si desidera, impostare i campi che seguono.
   a. `Autorizza URL endpoint` per specificare un URL di autorizzazione OAuth.

      Per `Autorizza URL endpoint`, il nome host può contenere il nome di un Sandbox o di un dominio personalizzato (creato mediante Dominio personale), ma l'URL deve finire con `.salesforce.com` e il percorso deve finire con `/services/oauth2/authorize`. Ad esempio, `https://test.salesforce.com/services/oauth2/authorize`.

   b. `URL endpoint token` per specificare un URL token OAuth.

      Per `URL endpoint token`, il nome host può contenere il nome di un Sandbox o di un dominio personalizzato (creato mediante Dominio personale), ma l'URL deve finire con `.salesforce.com` e il percorso deve finire con `/services/oauth2/token`. Ad esempio, `https://test.salesforce.com/services/oauth2/token`.

   c. `Ambiti predefiniti` da inviare insieme alla richiesta all'endpoint di autorizzazione. Se non si imposta il campo viene utilizzata l'impostazione predefinita codificata.

      Per ulteriori informazioni, vedere Uso del parametro Scope.

      Nota: quando si modificano le impostazioni di un provider di autenticazione Salesforce esistente, potrebbe essere possibile selezionare una casella di controllo per includere l'ID organizzazione per i link account di terze parti. Per i provider di autenticazione Salesforce impostati nel rilascio Summer '14 o in un rilascio precedente, l'identità dell'utente fornita da un'organizzazione non include l'ID organizzazione. Pertanto, l'organizzazione di destinazione non può fare distinzione fra utenti con lo stesso ID utente provenienti da due fonti diverse (ad esempio, due Sandbox). Selezionare questa casella di controllo se si dispone già di un'organizzazione con due utenti (uno da ciascun Sandbox) mappati allo stesso utente nell'organizzazione di destinazione e si desidera mantenere separate le identità. In caso contrario, non selezionare la casella di controllo. Dopo che è stata abilitata questa funzionalità, gli utenti devono approvare nuovamente il collegamento a tutti i loro link di terze parti. Questi link sono elencati nella sezione Link account di terze parti della pagina dei dettagli di un utente. Per i provider di autenticazione Salesforce creati nel rilascio Winter '15 e nei rilasci successivi, questa funzione è abilitata per impostazione predefinita e la casella di controllo non è visualizzata.

   d. `URL di errore personalizzato` utilizzato dal provider per segnalare eventuali errori.
   e. `URL di disconnessione personalizzato` per fornire una destinazione specifica agli utenti autenticati con il flusso Single Sign-On che si disconnettono. Usare questo campo per indirizzare gli utenti a una pagina di disconnessione con l'immagine aziendale o a una destinazione diversa dalla pagina di disconnessione predefinita di Salesforce. L'URL deve essere completo e dotato di prefisso `http` o `https`, ad esempio `https://acme.my.salesforce.com`.
9. Selezionare una classe Apex già esistente, ad esempio la classe `Handler registrazione`, o fare clic su `Crea automaticamente un modello di handler registrazione` per creare il modello di classe Apex per l'handler di registrazione. È necessario modificare questa classe di modelli per modificare il contenuto predefinito prima di utilizzarlo.

   Nota: per consentire a Salesforce di generare l'`URL inizializzazione Single Sign-On`, è necessario specificare una classe di handler registrazione.

10. Selezionare l'utente che esegue la classe di handler Apex per `Esegui registrazione come`. L'utente deve disporre dell'autorizzazione "Gestisci utenti". È richiesto un utente se è stata selezionata una classe di handler registrazione o se se ne sta creando automaticamente una.
11. Per utilizzare un portale con il provider, selezionare il portale dall'elenco a discesa Portale.
12. Utilizzare il campo `URL icona` per associare un percorso a un'icona da visualizzare come pulsante nella pagina di accesso di una comunità. L'icona è valida solo per una comunità, e non compare nella pagina di accesso dell'organizzazione Salesforce o nel dominio personalizzato creato con Dominio personale. Gli utenti fanno clic sul pulsante per accedere con il provider di autenticazione associato della comunità.

    È possibile specificare il percorso di un'immagine personalizzata, oppure copiare nel campo l'URL di una delle icone di esempio.

13. Fare clic su `Salva`.

    Prendere nota del valore degli URL di configurazione client. È necessario l'`URL di richiamata` per completare l'ultima fase e utilizzare l'`URL inizializzazione solo test` per verificare la configurazione. Assicurarsi inoltre di annotare l'`ID provider di autenticazione` poiché dovrà essere utilizzato con la classe Apex `Auth.AuthToken`.

14. Tornare alla definizione dell'applicazione connessa creata in precedenza (nella pagina Applicazioni di Imposta, fare clic sul nome dell'applicazione connessa) e incollare il valore dell'`URL di richiamata` del provider di autenticazione nel campo `URL di richiamata`.

Dopo la definizione del provider di autenticazione vengono generati alcuni URL di configurazione client:

- `URL inizializzazione solo test`: gli amministratori utilizzano questo URL per assicurarsi che il provider di terze parti sia impostato correttamente. L'amministratore apre l'URL in un browser, accede al provider di terze parti e viene di nuovo reindirizzato a Salesforce con una mappa di attributi.
- `URL inizializzazione Single Sign-On`: utilizzare questo URL per eseguire il Single Sign-On in Salesforce da un provider di terze parti (con credenziali di terze parti). L'utente finale apre questo URL in un browser e accede al provider di terze parti. Successivamente crea un nuovo utente oppure aggiorna un utente già esistente, quindi effettua l'accesso a Salesforce come tale utente.
- `URL di collegamento utente esistente`: utilizzare questo URL per collegare gli utenti Salesforce esistenti a un account di terze parti. L'utente finale apre questo URL in un browser, accede al provider di terze parti, accede a Salesforce e approva il link.
- `URL inizializzazione solo Oauth`: Utilizzare questo URL per ottenere token di accesso OAuth per una terza parte. Affinché il servizio di terzi ottenga il token, gli utenti devono eseguire l'autenticazione in Salesforce; questo flusso non è predisposto per una futura funzionalità di Single Sign-On.
- `URL di richiamata`: utilizzare l'URL di richiamata per l'endpoint che il provider di autenticazione richiama per la configurazione. Il provider di autenticazione deve reindirizzare all'`URL di richiamata` con le informazioni per ciascuno degli URL di configurazione client di cui sopra.

Gli URL di configurazione client supportano ulteriori parametri di richiesta che consentono di richiedere agli utenti di accedere a specifici siti, ottenere autorizzazioni personalizzate da terze parti o passare a un percorso specifico dopo l'autenticazione.

### Provare la connessione Single Sign-On

In un browser, aprire l'`URL inizializzazione solo test` nella pagina dei dettagli del provider di autenticazione. Sia l'organizzazione di autorizzazione che l'organizzazione di destinazione devono trovarsi nello stesso ambiente, ad esempio produzione o Sandbox.

VEDERE ANCHE:

Uso dei parametri di richiesta con URL di configurazione client

Informazioni sui provider di autenticazione esterni

## Configurazione di un provider di autenticazione OpenID Connect

EDIZIONI

Disponibile nelle versioni: Lightning Experience e Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:
- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:
- "Personalizza applicazione"

  E

  "Gestisci provider di autenticazione"

Come provider di autenticazione si può utilizzare qualsiasi applicazione Web di terzi che implementi il lato server del protocollo OpenID Connect, come Amazon, Google e PayPal.

Per configurare un provider di autenticazione OpenID è necessario eseguire queste operazioni:

1. Registrare l'applicazione, impostando Salesforce come dominio dell'applicazione.
2. Definire un provider di autenticazione OpenID Connect nell'organizzazione Salesforce.
3. Aggiornare l'applicazione in modo che utilizzi l'`URL di richiamata` generato da Salesforce come URL di richiamata.
4. Provare la connessione.

### Registrare un'applicazione OpenID Connect

Per poter configurare un'applicazione Web per l'organizzazione Salesforce è necessario registrarla presso il proprio provider di servizi. Il procedimento varia a seconda del provider di servizi. Ad esempio, per registrare una Google App, creare un ID client OAuth 2.0.

1. Registrare l'applicazione sul sito Web del provider di servizi.
2. Modificare le impostazioni dell'applicazione e impostare il dominio dell'applicazione (o l'`URL pagina iniziale`) su Salesforce.
3. Prendere nota di ID client e segreto client, oltre che di Autorizza URL endpoint, URL endpoint token e URL endpoint info utente, che dovrebbero essere disponibili nella documentazione del provider. Ecco alcuni dei più diffusi provider di servizi OpenID Connect:
   - Amazon
   - Google
   - PayPal

### Definire un provider OpenID Connect nell'organizzazione Salesforce

Per configurare l'applicazione nell'organizzazione Salesforce sono necessarie alcune informazioni dal provider (ID client e segreto client, oltre ad Autorizza URL endpoint, URL endpoint token e URL endpoint info utente).

1. Da Imposta, immettere *`Provider di autenticazione`* nella casella `Ricerca veloce`, quindi selezionare **Provider di autenticazione**.
2. Fare clic su **Nuovo**.
3. Selezionare OpenID Connect per `Tipo provider`.

4. Immettere un `Nome` per il provider.
5. Immettere il `Suffisso URL`. Viene utilizzato negli URL di configurazione client. Ad esempio, se il suffisso URL del provider è "MyOpenIDConnectProvider", l'URL Single Sign-On è simile a: `https://login.salesforce.com/auth/sso/00Dx00000000001/MyOpenIDConnectProvider`.
6. Utilizzare l'ID client del provider per il campo `Chiave consumatore`.
7. Utilizzare il segreto client del provider per il campo `Segreto consumatore`.
8. Immettere l'URL di base del provider per il campo `Autorizza URL endpoint`.

   Suggerimento: Se necessario è possibile aggiungere all'URL di base dei parametri della stringa di query. Ad esempio, per ottenere un token di aggiornamento da Google per l'accesso offline, utilizzare `https://accounts.google.com/o/oauth2/auth?access_type=offline&approval_prompt=force`. In questo caso specifico, il parametro `approval_prompt` aggiuntivo è necessario per chiedere all'utente di accettare l'azione di aggiornamento, in modo che Google continui a fornire token di aggiornamento dopo il primo token.

9. Immettere l'`URL endpoint token` del provider.
10. Se lo si desidera, impostare i campi che seguono.
    a. `URL endpoint info utente` del provider.
    b. `Emittente token`. Questo valore identifica l'origine del token di autenticazione nel formato *`https: URL`*. Se questo valore viene specificato, il provider deve includere un valore `id_token` nella risposta a una richiesta di token. Il valore `id_token` non è obbligatorio per il flusso token di aggiornamento (ma sarà convalidato da Salesforce se indicato).
    c. `Ambiti predefiniti` da inviare insieme alla richiesta all'endpoint di autorizzazione. In caso contrario vengono utilizzate le impostazioni predefinite codificate per il tipo di provider (per l'elenco delle impostazioni predefinite, vedere la documentazione per sviluppatori OpenID Connect).

       Per ulteriori informazioni, vedere Uso del parametro Scope.

11. È possibile selezionare `Invia token di accesso nell'intestazione` per far sì che il token sia inviato in un'intestazione anziché in una stringa di query.
12. Se lo si desidera, impostare i campi che seguono.
    a. `URL di errore personalizzato` utilizzato dal provider per segnalare eventuali errori.
    b. `URL di disconnessione personalizzato` per fornire una destinazione specifica agli utenti autenticati con il flusso Single Sign-On che si disconnettono. Usare questo campo per indirizzare gli utenti a una pagina di disconnessione con l'immagine aziendale o a una destinazione diversa dalla pagina di disconnessione predefinita di Salesforce. L'URL deve essere completo e dotato di prefisso `http` o `https`, ad esempio `https://acme.my.salesforce.com`.
    c. Selezionare una classe Apex esistente come classe `Handler registrazione` o fare clic su `Crea automaticamente un modello di handler registrazione` per creare un modello di classe Apex per l'handler di registrazione. È necessario modificare questa classe e il contenuto predefinito prima di utilizzarlo.

       Nota: per consentire a Salesforce di generare l'`URL inizializzazione Single Sign-On`, è necessario specificare una classe di handler registrazione.

    d. Selezionare l'utente che esegue la classe di handler Apex per **Esegui registrazione come**. L'utente deve disporre dell'autorizzazione "Gestisci utenti". È richiesto un utente se è stata selezionata una classe di handler registrazione o se se ne sta creando automaticamente una.
    e. Per utilizzare un portale con il provider, selezionare il portale dall'elenco a discesa Portale.

f. Utilizzare il campo `URL icona` per associare un percorso a un'icona da visualizzare come pulsante nella pagina di accesso di una comunità. L'icona è valida solo per una comunità, e non compare nella pagina di accesso dell'organizzazione Salesforce o nel dominio personalizzato creato con Dominio personale. Gli utenti fanno clic sul pulsante per accedere con il provider di autenticazione associato della comunità.

   È possibile specificare il percorso di un'immagine personalizzata, oppure copiare nel campo l'URL di una delle icone di esempio.

13. Fare clic su **Salva**.

Assicurarsi di annotare il valore `ID provider di autenticazione` generato. È necessario utilizzarlo con la classe Apex `Auth.AuthToken`.

Dopo la definizione del provider di autenticazione vengono generati alcuni URL di configurazione client:

- `URL inizializzazione solo test`: gli amministratori utilizzano questo URL per assicurarsi che il provider di terze parti sia impostato correttamente. L'amministratore apre l'URL in un browser, accede al provider di terze parti e viene di nuovo reindirizzato a Salesforce con una mappa di attributi.
- `URL inizializzazione Single Sign-On`: utilizzare questo URL per eseguire il Single Sign-On in Salesforce da un provider di terze parti (con credenziali di terze parti). L'utente finale apre questo URL in un browser e accede al provider di terze parti. Successivamente crea un nuovo utente oppure aggiorna un utente già esistente, quindi effettua l'accesso a Salesforce come tale utente.
- `URL di collegamento utente esistente`: utilizzare questo URL per collegare gli utenti Salesforce esistenti a un account di terze parti. L'utente finale apre questo URL in un browser, accede al provider di terze parti, accede a Salesforce e approva il link.
- `URL inizializzazione solo Oauth`: Utilizzare questo URL per ottenere token di accesso OAuth per una terza parte. Affinché il servizio di terzi ottenga il token, gli utenti devono eseguire l'autenticazione in Salesforce; questo flusso non è predisposto per una futura funzionalità di Single Sign-On.
- `URL di richiamata`: utilizzare l'URL di richiamata per l'endpoint che il provider di autenticazione richiama per la configurazione. Il provider di autenticazione deve reindirizzare all'`URL di richiamata` con le informazioni per ciascuno degli URL di configurazione client di cui sopra.

Gli URL di configurazione client supportano ulteriori parametri di richiesta che consentono di richiedere agli utenti di accedere a specifici siti, ottenere autorizzazioni personalizzate da terze parti o passare a un percorso specifico dopo l'autenticazione.

## Aggiornare l'applicazione OpenID Connect

Dopo avere definito il provider di autenticazione nell'organizzazione Salesforce, tornare al provider e aggiornare l'`URL di richiamata` dell'applicazione (noto anche come `Authorized Redirect URI` per le applicazioni Google e `Return URL` per PayPal).

## Provare la connessione Single Sign-On

In un browser, aprire l'`URL inizializzazione solo test` nella pagina dei dettagli del provider di autenticazione. Dovrebbe reindirizzare al servizio del provider e chiedere di effettuare l'accesso. Una volta effettuato l'accesso, viene richiesta l'autorizzazione dell'applicazione. Dopo avere concesso l'autorizzazione si è nuovamente indirizzati a Salesforce.

## Configurazione di un provider di autenticazione Microsoft® Access Control Service

È possibile utilizzare Microsoft Access Control Service come provider di autenticazione, con il protocollo OAuth. L'autenticazione in genere avviene mediante un servizio Microsoft Office 365 come SharePoint® Online.

Salesforce supporta l'autenticazione da Microsoft Access Control Service con l'uso del solo protocollo OAuth. L'autenticazione Single Sign-On da un provider di autenticazione Microsoft non è supportata.

Per configurare un provider di autenticazione Microsoft Access Control Service è necessario eseguire le operazioni seguenti:

1. Definire un provider di autenticazione Microsoft Access Control Service nell'organizzazione Salesforce.
2. Registrare l'applicazione su Microsoft, impostando Salesforce come dominio dell'applicazione.
3. Modificare i dettagli del provider di autenticazione Microsoft Access Control Service in Salesforce per utilizzare la `Chiave consumatore` e il `Segreto consumatore` generati quando l'applicazione è stata registrata su Microsoft.
4. Provare la connessione.

EDIZIONI

Disponibile nelle versioni: Lightning Experience e Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:
- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:
- "Personalizza applicazione"

  E

  "Gestisci provider di autenticazione"

### Definire un provider di autenticazione Microsoft Access Control Service nell'organizzazione Salesforce

Per poter registrare un'applicazione in SharePoint Online o nel Microsoft Seller Dashboard, è necessario l'URL di richiamata che sarà utilizzato per reindirizzare l'utente autorizzato a Salesforce.

1. Da Imposta, immettere *`Provider di autenticazione`* nella casella `Ricerca veloce`, quindi selezionare **Provider di autenticazione**.
2. Fare clic su **Nuovo**.
3. Selezionare Microsoft Access Control Service per il `Tipo provider`.
4. Immettere un `Nome` per il provider.
5. Immettere il `Suffisso URL`. Viene utilizzato negli URL di configurazione client. Ad esempio, se il suffisso URL del provider è "MyMicrosoftACSProvider", l'URL di richiamata è simile a:

   `https://login.salesforce.com/services/authcallback/00Dx00000000001/MyMicrosoftACSProvider`

6. Inserire un segnaposto per il valore del campo `Chiave consumatore` (valore che si modificherà dopo la registrazione dell'applicazione presso Microsoft).
7. Inserire un segnaposto per il valore del campo `Segreto consumatore` (valore che si modificherà dopo la registrazione dell'applicazione presso Microsoft).
8. Immettere l'URL di base del provider per il campo `Autorizza URL endpoint`. Ad esempio, SharePoint Online utilizza il seguente formato:

   `https://<sharepoint online host name>/_layouts/15/OAuthAuthorize.aspx`

9. Immettere l'`URL endpoint token` nel formato seguente.

   `https://accounts.accesscontrol.windows.net/<tenant>/tokens/OAuth/2?resource=<sender ID>/<sharepoint online host name>@<tenant>`

   - `<tenant>` è il nome tenant di Office 365 che termina con `.onmicrosoft.com` o il GUID (Globally Unique Identifier) del tenant corrispondente.

- `<sender ID>` è l'identificatore del mittente del token. Ad esempio, SharePoint utilizza `00000003-0000-0ff1-ce00-000000000000`

10. Se lo si desidera, impostare i campi che seguono.
    - `Ambiti predefiniti` da inviare insieme alla richiesta all'endpoint di autorizzazione. Per ulteriori informazioni sugli ambiti per SharePoint Online, vedere http://msdn.microsoft.com/en-us/library/jj687470.aspx#Scope o, per maggiori informazioni sull'uso degli ambiti con Salesforce, Uso del parametro Scope.
    - `URL di errore personalizzato` utilizzato dal provider per segnalare eventuali errori.
    - `URL di disconnessione personalizzato` per fornire una destinazione specifica agli utenti autenticati con il flusso Single Sign-On che si disconnettono. Usare questo campo per indirizzare gli utenti a una pagina di disconnessione con l'immagine aziendale o a una destinazione diversa dalla pagina di disconnessione predefinita di Salesforce. L'URL deve essere completo e dotato di prefisso `http` o `https`, ad esempio `https://acme.my.salesforce.com`.
    - Per utilizzare un portale con il provider, selezionare il portale dall'elenco a discesa `Portale`. Se per l'organizzazione è impostato un portale, questa opzione può reindirizzare la richiesta di accesso alla pagina di accesso del portale. In caso contrario, lasciare il campo impostato su *`Nessuno`*.
    - Utilizzare il campo `URL icona` per associare un percorso a un'icona da visualizzare come pulsante nella pagina di accesso di una comunità. L'icona è valida solo per una comunità, e non compare nella pagina di accesso dell'organizzazione Salesforce o nel dominio personalizzato creato con Dominio personale. Gli utenti fanno clic sul pulsante per accedere con il provider di autenticazione associato della comunità.

      È possibile specificare il percorso di un'immagine personalizzata, oppure copiare nel campo l'URL di una delle icone di esempio.

11. Fare clic su **Salva**.

Assicurarsi di annotare il valore `ID provider di autenticazione` generato. È possibile utilizzarlo con la classe Apex `Auth.AuthToken`.

Dopo la definizione del provider di autenticazione vengono generati alcuni URL di configurazione client:

- `URL inizializzazione solo test`: gli amministratori utilizzano questo URL per assicurarsi che il provider di terze parti sia impostato correttamente. L'amministratore apre l'URL in un browser, accede al provider di terze parti e viene di nuovo reindirizzato a Salesforce con una mappa di attributi.
- `URL inizializzazione solo Oauth`: Utilizzare questo URL per ottenere token di accesso OAuth per una terza parte. Affinché il servizio di terzi ottenga il token, gli utenti devono eseguire l'autenticazione in Salesforce; questo flusso non è predisposto per una futura funzionalità di Single Sign-On.
- `URL di richiamata`: utilizzare l'URL di richiamata per l'endpoint che il provider di autenticazione richiama per la configurazione. Il provider di autenticazione deve reindirizzare all'`URL di richiamata` con le informazioni per ciascuno degli URL di configurazione client di cui sopra.

Gli URL di configurazione client supportano ulteriori parametri di richiesta che consentono di richiedere agli utenti di accedere a specifici siti, ottenere autorizzazioni personalizzate da terze parti o passare a un percorso specifico dopo l'autenticazione.

## Registrare l'applicazione su Microsoft

Prima di configurare un'applicazione per un'organizzazione Salesforce è necessario ottenere un'identità per l'applicazione mediante una delle opzioni offerte da Microsoft. Per informazioni su come registrare un'applicazione remota per SharePoint, vedere ad esempio le Guidelines for registering apps for SharePoint 2013.

1. Registrare l'applicazione mediante una delle opzioni offerte da Microsoft.
2. Modificare le impostazioni dell'applicazione e impostare l'URI di reindirizzamento sull'`URL di richiamata` del provider di autenticazione.

3. Annotare l'`ID client` e il `Segreto client`.
4. Fare clic su **Salva**.

### Modificare i dettagli del provider di autenticazione Microsoft Access Control Service

Dopo avere registrato l'applicazione presso Microsoft, tornare ai dettagli del provider di autenticazione Microsoft Access Control Service e aggiornare la `Chiave consumatore` e il `Segreto consumatore` con i valori forniti da Microsoft.

1. Da Imposta, immettere *`Provider di autenticazione`* nella casella `Ricerca veloce`, quindi selezionare **Provider di autenticazione**.
2. Fare clic su **Modifica** accanto al nome del provider di autenticazione Microsoft Access Control Service.
3. Immettere il valore dell'`ID client` fornito da Microsoft nel campo `Chiave consumatore`.
4. Immettere il valore del `Segreto client` fornito da Microsoft nel campo `Segreto consumatore`.

### Provare la connessione

In un browser, aprire l'`URL inizializzazione solo test` nella pagina dei dettagli del provider di autenticazione. Dovrebbe reindirizzare al servizio del provider e chiedere di effettuare l'accesso. Una volta effettuato l'accesso, viene richiesta l'autorizzazione dell'applicazione. Dopo avere concesso l'autorizzazione si è nuovamente indirizzati a Salesforce.

## Configurazione di un provider di autenticazione LinkedIn

Consente agli utenti di accedere a un'organizzazione Salesforce con il loro account LinkedIn.

Per configurare LinkedIn come provider di autenticazione, eseguire le operazioni indicate di seguito.

1. Decidere quali ambiti (dettagli utente) ottenere da LinkedIn.
2. Impostare un'applicazione LinkedIn.
3. Definire un provider LinkedIn nell'organizzazione Salesforce e stabilire un handler registrazione.
4. Modificare l'handler registrazione.
5. Aggiornare l'applicazione LinkedIn per utilizzare l'URL di richiamata generato da Salesforce come valore da inserire negli `URL di reindirizzamento OAuth 2.0` di LinkedIn.
6. Provare la connessione Single Sign-On.

EDIZIONI

Disponibile nelle versioni: Lightning Experience e Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:
- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:
- "Personalizza applicazione"

  E

  "Gestisci provider di autenticazione"

### Decidere quali ambiti (dettagli utente) ottenere da LinkedIn

Gli ambiti determinano le informazioni su un utente ottenute tramite LinkedIn durante il processo di autorizzazione. È possibile richiedere alcune informazioni di base come il nome utente e l'URL di una fotografia, oppure informazioni più specifiche come un indirizzo, un numero di telefono, un elenco di referenti e così via. L'utente approva lo scambio di informazioni prima che queste vengano trasmesse.

Quando si configura LinkedIn come provider di autenticazione è possibile impostare gli ambiti in tre punti diversi: nelle impostazioni dell'applicazione LinkedIn, nelle impostazioni del provider di autenticazione Salesforce o in una query diretta all'endpoint info utente di LinkedIn mediante selettori di campi. Nel decidere dove specificare gli ambiti e i valori da utilizzare, prestare attenzione ai seguenti punti.

- È possibile non specificare questo valore nelle impostazioni di LinkedIn e di Salesforce. Il valore predefinito è *r_basicprofile*, che fornisce solo le informazioni più generiche sull'utente definite da LinkedIn.
- Salesforce richiede l'indirizzo email per gli utenti.
- Per un elenco dei valori supportati e del loro significato, consultare la documentazione di LinkedIn relativa all'autenticazione; oppure, per informazioni sulla richiesta degli ambiti mediante un URL, consultare la pagina relativa ai selettori di pagina in LinkedIn.
- Se si configurano gli Ambiti predefiniti nelle impostazioni del provider di autenticazione Salesforce, quel valore ha la precedenza sul valore indicato nelle impostazioni dell'applicazione LinkedIn.
- Se nelle impostazioni dell'applicazione LinkedIn o nelle impostazioni del provider di autenticazione Salesforce si indicano più ambiti, separare i valori con un solo spazio, ad esempio *r_basicprofile r_emailaddress*.
- Se si utilizzano i selettori di campo LinkedIn con un URL, separare i valori con una sola virgola, ad esempio `https://api.linkedin.com/v1/people/~:(id,formatted-name,first-name,last-name,public-profile-url,email-address)`.

## Impostare un'applicazione LinkedIn

Per poter configurare LinkedIn per l'organizzazione Salesforce, impostare un'applicazione in LinkedIn.

Nota: questo passaggio si può saltare consentendo a Salesforce di usare l'applicazione predefinita. Per ulteriori informazioni, vedere Uso dei valori gestiti da Salesforce nell'impostazione dei provider di autenticazione.

1. Accedere all'account sviluppatore per il sito LinkedIn.
2. Fare clic sul nome utente in alto e selezionare **API Keys**.
3. Fare clic su **Aggiungi una nuova applicazione**.
4. Specificare le impostazioni dell'applicazione.
5. Prendere nota della Chiave API e della Chiave segreta della nuova applicazione che verranno utilizzate in seguito in Salesforce.
6. Se si desidera, inserire un valore di ambito supportato da LinkedIn o più valori separati da uno spazio.

   Per ulteriori informazioni sull'uso degli ambiti con LinkedIn, vedere Decidere quali ambiti (dettagli utente) ottenere da LinkedIn.

## Definire un provider LinkedIn nell'organizzazione Salesforce

Per impostare un provider LinkedIn nell'organizzazione Salesforce sono necessarie la `Chiave API` e la `Chiave segreta`.

Nota: è possibile evitare di specificare questi valori chiave nell'impostazione del provider affidando a Salesforce la gestione dei valori. Per ulteriori informazioni, vedere Uso dei valori gestiti da Salesforce nell'impostazione dei provider di autenticazione.

1. Da Imposta, immettere *Provider di autenticazione* nella casella `Ricerca veloce`, quindi selezionare **Provider di autenticazione**.
2. Fare clic su **Nuovo**.
3. Selezionare LinkedIn per `Tipo provider`.
4. Immettere un `Nome` per il provider.
5. Immettere il `Suffisso URL`. Viene utilizzato negli URL di configurazione client. Ad esempio, se il suffisso URL del provider è "MyLinkedInProvider", l'URL Single Sign-On è simile a:

   `https://login.salesforce.com/services/sso/00Dx00000000001/MyLinkedInProvider`

6. Utilizzare la `Chiave API` di LinkedIn per il campo `Chiave consumatore`.
7. Utilizzare la `Chiave segreta` di LinkedIn per il campo `Segreto consumatore`.
8. Se si desidera, impostare i campi che seguono.

a. `Autorizza URL endpoint` per immettere l'URL di autorizzazione di base da LinkedIn. Ad esempio, `https://www.linkedin.com/uas/oauth2/authorization/auth`. L'URL deve iniziare con *`https://www.linkedin.com/uas/oauth2/authorization`*.

> Suggerimento: Se necessario è possibile aggiungere all'URL di base dei parametri della stringa di query. Ad esempio, per ottenere un token di aggiornamento da Google per l'accesso offline, utilizzare `https://accounts.google.com/o/oauth2/auth?access_type=offline&approval_prompt=force`. Il parametro `approval_prompt` è necessario per chiedere all'utente di accettare l'azione di aggiornamento, in modo che Google continui a fornire token di aggiornamento dopo il primo token.

b. `Url endpoint token` per immettere l'URL token OAuth da LinkedIn. Ad esempio, `https://www.linked.com/uas/oauth2/accessToken/token`. L'URL deve iniziare con *`https://www.linkedin.com/uas/oauth2/accessToken`*.

c. `URL endpoint info utente` per modificare i valori richiesti dall'API del profilo LinkedIn. Per ulteriori informazioni, vedere https://developer.linkedin.com/documents/profile-fields. L'URL deve iniziare con *`https://api.linkedin.com/v1/people/~`* e i campi richiesti devono corrispondere agli ambiti richiesti.

d. `Ambiti predefiniti` per immettere un valore supportato o più valori separati da uno spazio che rappresentano le informazioni ottenute da LinkedIn. Per ulteriori informazioni, vedere Decidere quali ambiti (dettagli utente) ottenere da LinkedIn.

e. `URL di errore personalizzato` utilizzato dal provider per segnalare eventuali errori.

f. `URL di disconnessione personalizzato` per fornire una destinazione specifica agli utenti autenticati con il flusso Single Sign-On che si disconnettono. Usare questo campo per indirizzare gli utenti a una pagina di disconnessione con l'immagine aziendale o a una destinazione diversa dalla pagina di disconnessione predefinita di Salesforce. L'URL deve essere completo e dotato di prefisso `http` o `https`, ad esempio `https://acme.my.salesforce.com`.

g. Fare clic su **Crea automaticamente un modello di handler registrazione** per creare un modello di classe Apex per l'handler di registrazione, se non ne è già presente uno. In seguito, modificare questa classe e modificare il contenuto predefinito prima di utilizzarlo.

> Nota: specificare una classe di handler registrazione per consentire a Salesforce di generare l'URL inizializzazione Single Sign-On.

h. Selezionare l'utente che esegue la classe di handler Apex per `Esegui registrazione come`. L'utente deve disporre dell'autorizzazione "Gestisci utenti". È richiesto un utente se è stata selezionata una classe di handler registrazione o se se ne sta creando automaticamente una.

i. Per utilizzare un portale per gli utenti LinkedIn, selezionarlo dall'elenco a discesa Portale.

9. Utilizzare il campo `URL icona` per associare un percorso a un'icona da visualizzare come pulsante nella pagina di accesso di una comunità. L'icona è valida solo per una comunità, e non compare nella pagina di accesso dell'organizzazione Salesforce o nel dominio personalizzato creato con Dominio personale. Gli utenti fanno clic sul pulsante per accedere con il provider di autenticazione associato della comunità.

   È possibile specificare il percorso di un'immagine personalizzata, oppure copiare nel campo l'URL di una delle icone di esempio.

10. Fare clic su **Salva**.

Dopo la definizione del provider di autenticazione vengono generati alcuni URL di configurazione client:

- `URL inizializzazione solo test`: gli amministratori utilizzano questo URL per assicurarsi che il provider di terze parti sia impostato correttamente. L'amministratore apre l'URL in un browser, accede al provider di terze parti e viene di nuovo reindirizzato a Salesforce con una mappa di attributi.
- `URL inizializzazione Single Sign-On`: utilizzare questo URL per eseguire il Single Sign-On in Salesforce da un provider di terze parti (con credenziali di terze parti). L'utente finale apre questo URL in un browser e accede al provider di terze parti.

Successivamente crea un nuovo utente oppure aggiorna un utente già esistente, quindi effettua l'accesso a Salesforce come tale utente.

- `URL di collegamento utente esistente`: utilizzare questo URL per collegare gli utenti Salesforce esistenti a un account di terze parti. L'utente finale apre questo URL in un browser, accede al provider di terze parti, accede a Salesforce e approva il link.
- `URL inizializzazione solo Oauth`: Utilizzare questo URL per ottenere token di accesso OAuth per una terza parte. Affinché il servizio di terzi ottenga il token, gli utenti devono eseguire l'autenticazione in Salesforce; questo flusso non è predisposto per una futura funzionalità di Single Sign-On.
- `URL di richiamata`: utilizzare l'URL di richiamata per l'endpoint che il provider di autenticazione richiama per la configurazione. Il provider di autenticazione deve reindirizzare all'`URL di richiamata` con le informazioni per ciascuno degli URL di configurazione client di cui sopra.

Gli URL di configurazione client supportano ulteriori parametri di richiesta che consentono di richiedere agli utenti di accedere a specifici siti, ottenere autorizzazioni personalizzate da terze parti o passare a un percorso specifico dopo l'autenticazione.

## Modificare l'handler registrazione

1. Da Imposta, immettere *`Classi Apex`* nella casella `Ricerca veloce`, quindi selezionare **Classi Apex**.
2. Modificare l'handler di registrazione Apex creato automaticamente (oppure l'handler di registrazione esistente, se presente) per mappare i campi fra LinkedIn e Salesforce

   Nota: la query profilo predefinita per LinkedIn recupera solo i campi seguenti: first-name, last-name, headline, profile URL. Per l'handler di registrazione predefinito è necessario l'indirizzo email. Eliminare la necessità di indicare l'email dall'handler di registrazione o modificare gli ambiti desiderati in Decidere quali ambiti (dettagli utente) ottenere da LinkedIn per includere l'indirizzo email e altri eventuali campi nell'handler di registrazione.

   Di seguito è riportato un esempio di handler di registrazione Apex specifico per un'applicazione LinkedIn come provider di autenticazione. L'handler di registrazione presuppone che gli ambiti richiesti comprendano *`r_basicprofile`* e *`r_emailaddress`*. Presuppone inoltre che gli utenti eseguano l'accesso a un Portale Clienti.

```
//TODO:This auto-generated class includes the basics for a Registration
//Handler class. You will need to customize it to ensure it meets your needs and
//the data provided by the third party.
global class LinkedInRegHandler implements Auth.RegistrationHandler {
    //Creates a Standard salesforce or a community user
    global User createUser(Id portalId, Auth.UserData data) {
        if (data.attributeMap.containsKey('sfdc_networkid')) {
            //We have a community id, so create a user with community access
            //TODO: Get an actual account
            Account a =[SELECT Id FROM account WHERE name = 'LinkedIn Account'];
            Contact c = new Contact();
            c.accountId = a.Id;
            c.email = data.email;
            c.firstName = data.firstName;
            c.lastName = data.lastName;
            insert(c);
            //TODO: Customize the username and profile. Also check that the username
            //doesn't already exist and possibly ensure there are enough org licenses
            //to create a user. Must be 80 characters or less.
            User u = new User();
            Profile p =[SELECT Id FROM profile WHERE name = 'Customer Portal Manager'];

            u.username = data.firstName + '@sfdc.linkedin.com';
```

```
            u.email = data.email;
            u.lastName = data.lastName;
            u.firstName = data.firstName;
            String alias = data.firstName;
            //Alias must be 8 characters or less
            if (alias.length() > 8) {
                alias = alias.substring(0, 8);
            }
            u.alias = alias;
            u.languagelocalekey = UserInfo.getLocale();
            u.localesidkey = UserInfo.getLocale();
            u.emailEncodingKey = 'UTF-8';
            u.timeZoneSidKey = 'America/Los_Angeles';
            u.profileId = p.Id;
            u.contactId = c.Id;
            return u;
        } else {
            //This is not a community, so create a regular standard user
            User u = new User();
            Profile p =[SELECT Id FROM profile WHERE name = 'Standard User'];
            //TODO: Customize the username. Also check that the username doesn't
            //already exist and possibly ensure there are enough org licenses
            //to create a user. Must be 80 characters or less
            u.username = data.firstName + '@salesforce.com';
            u.email = data.email;
            u.lastName = data.lastName;
            u.firstName = data.firstName;
            String alias = data.firstName;
            //Alias must be 8 characters or less
            if (alias.length() > 8) {
                alias = alias.substring(0, 8);
            }
            u.alias = alias;
            u.languagelocalekey = UserInfo.getLocale();
            u.localesidkey = UserInfo.getLocale();
            u.emailEncodingKey = 'UTF-8';
            u.timeZoneSidKey = 'America/Los_Angeles';
            u.profileId = p.Id;
            return u;
        }
    }
    //Updates the user's first and last name
    global void updateUser(Id userId, Id portalId, Auth.UserData data) {
        User u = new User(id = userId);
        u.lastName = data.lastName;
        u.firstName = data.firstName;
        update(u);
    }
}
```

Per ulteriori informazioni ed esempi, vedere la documentazione dell'interfaccia RegistrationHandler.

### Aggiornare l'applicazione LinkedIn

Dopo avere definito il provider di autenticazione LinkedIn nell'organizzazione Salesforce, tornare a LinkedIn e aggiornare l'applicazione per utilizzare l'`URL di richiamata` generato da Salesforce come valore degli `URL di reindirizzamento OAuth 2.0` di LinkedIn.

### Provare la connessione Single Sign-On

In un browser, aprire l'`URL inizializzazione solo test` nella pagina dei dettagli del provider di autenticazione. Dovrebbe reindirizzare a LinkedIn e chiedere di effettuare l'accesso. Una volta effettuato l'accesso, viene richiesta l'autorizzazione dell'applicazione. Dopo avere concesso l'autorizzazione si è nuovamente indirizzati a Salesforce.

## Configurazione di un provider di autenticazione Twitter

Consente agli utenti di accedere a un'organizzazione Salesforce con il loro account Twitter.

Per configurare Twitter come provider di autenticazione, eseguire le operazioni indicate di seguito.

1. Impostare un'applicazione Twitter.
2. Definire un provider Twitter nell'organizzazione Salesforce e stabilire un handler registrazione.
3. Modificare l'handler registrazione.
4. Aggiornare l'applicazione Twitter per utilizzare l'URL di richiamata generato da Salesforce come valore da inserire nelle impostazioni dell'applicazione Twitter.
5. Provare la connessione Single Sign-On.

EDIZIONI

Disponibile nelle versioni: Lightning Experience e Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:
- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:
- "Personalizza applicazione"

  E

  "Gestisci provider di autenticazione"

### Impostare un'applicazione Twitter

Per poter configurare Twitter per l'organizzazione Salesforce, è necessario prima impostare un'applicazione in Twitter.

Nota: questo passaggio si può saltare consentendo a Salesforce di usare l'applicazione predefinita. Per ulteriori informazioni, vedere Uso dei valori gestiti da Salesforce nell'impostazione dei provider di autenticazione.

1. Accedere all'account sviluppatore per il sito di Twitter.
2. Fare clic sull'icona dell'utente in alto e selezionare **My Applications** (o accedere ad apps.twitter.com).
3. Fare clic su **Create New App**.
4. Specificare le impostazioni dell'applicazione.
5. Nelle API Keys, prendere nota della `Chiave API` e del `Segreto API` della nuova applicazione, che saranno necessari in seguito in Salesforce.

### Definire un provider Twitter nell'organizzazione Salesforce

Per impostare un provider Twitter nell'organizzazione Salesforce sono necessari la `Chiave API` e il `Segreto API` dell'applicazione Twitter.

Nota: è possibile evitare di specificare questi valori chiave nell'impostazione del provider affidando a Salesforce la gestione dei valori. Per ulteriori informazioni, vedere Uso dei valori gestiti da Salesforce nell'impostazione dei provider di autenticazione.

1. Da Imposta, immettere `Provider di autenticazione` nella casella `Ricerca veloce`, quindi selezionare **Provider di autenticazione**.
2. Fare clic su **Nuovo**.
3. Selezionare Twitter per `Tipo provider`.
4. Immettere un `Nome` per il provider.
5. Immettere il `Suffisso URL`. Viene utilizzato negli URL di configurazione client. Ad esempio, se il suffisso URL del provider è "MyTwitterProvider", l'URL Single Sign-On è simile a:

   `https://login.salesforce.com/services/sso/00Dx00000000001/MyTwitterProvider`

6. Utilizzare la `Chiave API` di Twitter per il campo `Chiave consumatore`.
7. Utilizzare il `Segreto API` di Twitter per il campo `Segreto consumatore`.
8. Se lo si desidera, impostare i campi che seguono
   a. `URL di errore personalizzato` utilizzato dal provider per segnalare eventuali errori.
   b. `URL di disconnessione personalizzato` per fornire una destinazione specifica agli utenti autenticati con il flusso Single Sign-On che si disconnettono. Usare questo campo per indirizzare gli utenti a una pagina di disconnessione con l'immagine aziendale o a una destinazione diversa dalla pagina di disconnessione predefinita di Salesforce. L'URL deve essere completo e dotato di prefisso `http` o `https`, ad esempio `https://acme.my.salesforce.com`.
   c. Fare clic su **Crea automaticamente un modello di handler registrazione** per creare un modello di classe Apex per l'handler di registrazione, se non ne è già presente uno. In seguito sarà necessario modificare questa classe, e modificare il contenuto predefinito prima di utilizzarlo.

      Nota: per consentire a Salesforce di generare l'URL inizializzazione Single Sign-On, è necessario specificare una classe di handler registrazione.

   d. Selezionare l'utente che esegue la classe di handler Apex per `Esegui registrazione come`. L'utente deve disporre dell'autorizzazione "Gestisci utenti". È richiesto un utente se è stata selezionata una classe di handler registrazione o se se ne sta creando automaticamente una.
   e. Per utilizzare un portale per gli utenti Twitter, selezionarlo dall'elenco a discesa Portale.
   f. Utilizzare il campo `URL icona` per associare un percorso a un'icona da visualizzare come pulsante nella pagina di accesso di una comunità. L'icona è valida solo per una comunità, e non compare nella pagina di accesso dell'organizzazione Salesforce o nel dominio personalizzato creato con Dominio personale. Gli utenti fanno clic sul pulsante per accedere con il provider di autenticazione associato della comunità.

      È possibile specificare il percorso di un'immagine personalizzata, oppure copiare nel campo l'URL di una delle icone di esempio.

9. Fare clic su **Salva**.

Dopo la definizione del provider di autenticazione vengono generati alcuni URL di configurazione client:

- `URL inizializzazione solo test`: gli amministratori utilizzano questo URL per assicurarsi che il provider di terze parti sia impostato correttamente. L'amministratore apre l'URL in un browser, accede al provider di terze parti e viene di nuovo reindirizzato a Salesforce con una mappa di attributi.
- `URL inizializzazione Single Sign-On`: utilizzare questo URL per eseguire il Single Sign-On in Salesforce da un provider di terze parti (con credenziali di terze parti). L'utente finale apre questo URL in un browser e accede al provider di terze parti. Successivamente crea un nuovo utente oppure aggiorna un utente già esistente, quindi effettua l'accesso a Salesforce come tale utente.

- `URL di collegamento utente esistente`: utilizzare questo URL per collegare gli utenti Salesforce esistenti a un account di terze parti. L'utente finale apre questo URL in un browser, accede al provider di terze parti, accede a Salesforce e approva il link.
- `URL di richiamata`: utilizzare l'URL di richiamata per l'endpoint che il provider di autenticazione richiama per la configurazione. Il provider di autenticazione deve reindirizzare all'`URL di richiamata` con le informazioni per ciascuno degli URL di configurazione client di cui sopra.

Gli URL di configurazione client supportano ulteriori parametri di richiesta che consentono di richiedere agli utenti di accedere a specifici siti, ottenere autorizzazioni personalizzate da terze parti o passare a un percorso specifico dopo l'autenticazione.

## Modificare l'handler registrazione

1. Da Imposta, immettere *`Classi Apex`* nella casella `Ricerca veloce`, quindi selezionare **Classi Apex**.
2. Modificare l'handler di registrazione Apex creato automaticamente (oppure l'handler di registrazione esistente, se presente) per mappare i campi fra Twitter e Salesforce

   Di seguito è riportato un esempio di handler di registrazione Apex specifico per un'applicazione Twitter come provider di autenticazione.

```
global class MyTwitterRegHandler implements Auth.RegistrationHandler{

global User createUser(Id portalId, Auth.UserData data)
{
    if(data.attributeMap.containsKey('sfdc_networkid'))
    {
        // Create communities user
        Account a = [SELECT Id FROM account WHERE name='Twitter Account']; // Make sure
 this account exists

        Contact c = new Contact();
        c.accountId = a.Id;
        c.email = 'temp@CHANGE-ME.com';
        c.firstName = data.fullname.split(' ')[0];
        c.lastName  = data.fullname.split(' ')[1];
        insert(c);

        User u = new User();
        Profile p = [SELECT Id FROM profile WHERE name='Customer Portal Manager'];
        u.username = data.username + '@sfdc-portal-twitter.com';
        u.email = 'temp@CHANGE-ME.com';
        u.firstName = data.fullname.split(' ')[0];
        u.lastName = data.fullname.split(' ')[1];
        String alias = data.fullname;

        //Alias must be 8 characters or less
        if(alias.length() > 8) {
            alias = alias.substring(0, 8);
    }

    u.alias = alias;
    u.languagelocalekey = 'en_US';
    u.localesidkey = 'en_US';
    u.emailEncodingKey = 'UTF-8';
    u.timeZoneSidKey = 'America/Los_Angeles';
    u.profileId = p.Id;
```

```
        u.contactId = c.Id;
        return u;
    } else {
        // Create Standard SFDC user
        User u = new User();
        Profile p = [SELECT Id FROM profile WHERE name='Standard User'];
        u.username = data.username + '@sfdc-twitter.com';
        u.email = 'temp@CHANGE-ME.com';
        u.firstName = data.fullname.split(' ')[0];
        u.lastName = data.fullname.split(' ')[1];
        String alias = data.fullname;
        if(alias.length() > 8)
            alias = alias.substring(0, 8);

        u.alias = alias;
        u.languagelocalekey = 'en_US';
        u.localesidkey = 'en_US';
        u.emailEncodingKey = 'UTF-8';
        u.timeZoneSidKey = 'America/Los_Angeles';
        u.profileId = p.Id;
        return u;
    }
}

global void updateUser(Id userId, Id portalId, Auth.UserData data)
{
        User u = new User(id=userId);
        u.firstName = data.fullname.split(' ')[0];
        u.lastName = data.fullname.split(' ')[1];
        String alias = data.fullname;
        if(alias.length() > 8)
            alias = alias.substring(0, 8);

        u.alias = alias;
        update(u);
}
}
```

Per ulteriori informazioni ed esempi, vedere la documentazione dell'interfaccia RegistrationHandler.

## Aggiornare l'applicazione Twitter

Dopo avere definito il provider di autenticazione Twitter nell'organizzazione Salesforce, tornare a Twitter e aggiornare l'applicazione per utilizzare l'`URL di richiamata` generato da Salesforce come valore dell'`URL di reindirizzamento` nelle impostazioni dell'applicazione Twitter.

Nota: nell'applicazione Twitter, selezionare **Allow this application to be used to Sign In with Twitter**.

## Provare la connessione Single Sign-On

In un browser, aprire l'`URL inizializzazione solo test` nella pagina dei dettagli del provider di autenticazione. Dovrebbe reindirizzare a Twitter e chiedere di effettuare l'accesso. Una volta effettuato l'accesso, viene richiesta l'autorizzazione dell'applicazione. Dopo avere concesso l'autorizzazione si è nuovamente indirizzati a Salesforce.

## Uso dei valori gestiti da Salesforce nell'impostazione dei provider di autenticazione

EDIZIONI

Disponibile nelle versioni: Lightning Experience e Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:

- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:

- "Personalizza applicazione"

  E

  "Gestisci provider di autenticazione"

È possibile decidere di lasciare che sia Salesforce a creare automaticamente i valori chiave durante l'impostazione di un provider di autenticazione Facebook, Salesforce, LinkedIn, Twitter o Google. In questo modo si evita di dover creare una propria applicazione di terzi.

Quando si decide di usare i valori gestiti da Salesforce nell'impostazione del provider di autenticazione, Salesforce utilizza l'applicazione predefinita in background da cui genera i valori, evitando all'utente di dover creare una propria applicazione.

Per utilizzare i valori gestiti da Salesforce, lasciare vuoti tutti i campi seguenti se sono visualizzati nell'impostazione del provider di autenticazione.

- `Chiave consumatore`
- `Segreto consumatore`
- `Autorizza URL endpoint`
- `URL endpoint token`
- `URL endpoint info utente`
- `Ambiti predefiniti`

Se si specifica un valore per uno dei campi precedenti, questo indica che si utilizza un'applicazione di terzi o un'applicazione connessa propria ed è necessario specificare i valori della `Chiave consumatore` e del `Segreto consumatore`.

Esempio: Si immagini di voler impostare il Single Sign-On con un provider di autenticazione LinkedIn per abilitare l'accesso a Salesforce con le credenziali di LinkedIn. Si può evitare di creare un'applicazione LinkedIn, poiché si è deciso di utilizzare i valori creati da Salesforce nell'impostazione del provider di autenticazione. Quindi, si definisce il provider di autenticazione LinkedIn nell'organizzazione e si prova la connessione con la procedura descritta in Configurazione di un provider di autenticazione LinkedIn.

## Uso di Frontdoor.jsp per accedere a Salesforce

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

È possibile utilizzare frontdoor.jsp per consentire agli utenti di accedere a Salesforce da un'interfaccia Web personalizzata (ad esempio un sito Force.com di accesso remoto o un'altra integrazione API) utilizzando l'ID sessione esistente e l'URL del server.

Per autenticare gli utenti con frontdoor.jsp, è necessario passare l'URL del server e l'ID completo della sessione (non l'ID di 15 o 18 caratteri) a frontdoor.jsp.

Il modo migliore di passare i valori è tramite un modulo che utilizza una richiesta `POST`. Ad esempio, il modulo seguente pubblica l'ID sessione corrente per frontdoor.jsp.

```
<form method="POST" action="https://instance.salesforce.com/secur/frontdoor.jsp">
<input type="hidden" name="sid"
      value="full_sessionID_value"
      />
<input type="submit" name="login" value="Log In" /></form>
```

È inoltre possibile inviare i valori come parametri URL, ma questo approccio non è sicuro quanto una richiesta `POST` perché espone l'ID sessione nell'URL.

```
https://instance.salesforce.com/secur/frontdoor.jsp?sid=full_sessionID_value
&retURL=optional_relative_url_to_open
```

Per le organizzazioni che utilizzano un dominio personalizzato creato con Dominio personale, è necessario passare il nome di dominio nell'URL del server.

Il modulo seguente pubblica l'ID sessione corrente per frontdoor.jsp per un dominio personalizzato.

```
<form method="POST" action="https://domain_name.my.salesforce.com/secur/frontdoor.jsp">
<input type="hidden" name="sid"
      value="full_sessionID_value"
      />
<input type="submit" name="login" value="Log In" /></form>
```

L'esempio che segue invia i valori come parametri URL.

```
https://domain_name.my.salesforce.com/secur/frontdoor.jsp?sid=full_sessionID_value
&retURL=optional_relative_url_to_open
```

## Istanza

È necessario conoscere l'istanza dell'organizzazione dell'utente. Ad esempio, se il `serverUrl` restituito quando si accede tramite l'API è `https://na1.salesforce.com`, na1 è l'istanza. La parte restante dell'indirizzo del server (il nome di dominio `salesforce.com`) resta uguale.

Se si crea un'integrazione per una singola organizzazione Salesforce, questo valore si può inserire direttamente nel codice. Se si crea un'integrazione per più organizzazioni, analizzare l'istanza dal `serverUrl` del `LoginResult` restituito dalla chiamata `login()` dell'API SOAP.

## ID sessione completo

L'ID sessione completo si può ottenere:

- Dall'`access_token` di un'autenticazione OAuth

  Suggerimento: Uno degli ambiti specificati quando si crea un'applicazione connessa deve essere Web o completo.

- Dal `LoginResult` restituito da una chiamata `login()` dell'API SOAP
- Da `UserInfo.getSessionId()` Apex

L'ID sessione restituito quando si utilizza il `{!GETSESSIONID()}` Visualforce non si può utilizzare con frontdoor.jsp.

Nota: Con frontdoor.jsp, non sono supportati tutti i tipi di sessione, ad esempio le sessioni API comunità. Per queste sessioni, considerare la possibilità di utilizzare SAML per Single Sign-On.

## URL relativo da aprire

È possibile includere un percorso relativo codificato nell'URL per reindirizzare gli utenti all'interfaccia utente di Salesforce o a un determinato record, oggetto, rapporto o pagina Visualforce (ad esempio, `/apex/MiaPaginaVisualforce`).

## Uso dei parametri di richiesta con URL di configurazione client

È possibile aggiungere funzionalità al provider di autenticazione utilizzando parametri di richiesta aggiuntivi.

I provider di autenticazione supportano ulteriori parametri di richiesta che consentono di richiedere agli utenti di accedere a specifici siti, ottenere autorizzazioni personalizzate da terze parti o passare a un percorso specifico dopo l'autenticazione.

Aggiungere i parametri di richiesta ai seguenti URL di configurazione client. Gli URL sono stati generati dopo la definizione del provider di autenticazione:

- URL inizializzazione solo test
- URL inizializzazione Single Sign-On
- URL di collegamento utente esistente
- URL di richiamata

Aggiungere uno dei seguenti parametri all'URL in base alle proprie esigenze. Per i provider Janrain, aggiungerli all'URL di richiamata appropriato.

- Scope – Personalizza le autorizzazioni richieste da terze parti
- Site – Consente di utilizzare il provider con un sito
- StartURL – Invia l'utente a un indirizzo specifico dopo l'autenticazione
- Community – Indirizza l'utente a una comunità specifica dopo l'autenticazione
- Authorization Endpoint a pagina 628 – Invia l'utente a un endpoint specifico per l'autenticazione (solo provider di autenticazione Salesforce)

EDIZIONI

Disponibile nelle versioni: Lightning Experience e Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:

- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:

- "Personalizza applicazione"

  E

  "Gestisci provider di autenticazione"

## Uso del parametro Scope

Consente di personalizzare le autorizzazioni richieste da terze parti come Facebook o Janrain in modo che il token di accesso restituito includa autorizzazioni aggiuntive.

È possibile personalizzare le richieste a terze parti per ricevere token di accesso con autorizzazioni aggiuntive. Vengono quindi utilizzati i metodi `Auth.AuthToken` per richiamare il token di accesso concesso in modo da consentire l'uso di tali autorizzazioni con terze parti.

Gli ambiti predefiniti variano a seconda delle terze parti, ma in genere consentono l'accesso solo alle informazioni utente di base. Ogni tipo di provider (OpenID Connect, Facebook, Salesforce e altri) ha una serie di ambiti predefiniti che invia insieme alla richiesta all'endpoint di autorizzazione. Ad esempio, l'ambito predefinito di Salesforce è `id`.

Gli ambiti si possono inviare in una stringa delimitata da spazi. La stringa delimitata da spazi degli ambiti richiesti viene inviata così com'è alle terze parti e ignora le autorizzazioni predefinite richieste dai provider di autenticazione.

Janrain non utilizza questo parametro; in Janrain è necessario configurare ulteriori autorizzazioni.

**Esempio:** Di seguito è riportato un esempio di parametro `scope` che richiede gli ambiti di Salesforce `api` e `web` aggiunti all'`URL inizializzazione Single Sign-On`, dove:

- *`orgID`* è l'ID del provider di autorizzazione
- *`URLsuffix`* è il valore specificato nella definizione del provider di autenticazione

```
https://login.salesforce.com/services/auth/sso/orgID/URLsuffix?scope=id%20api%20web
```

Poiché gli ambiti validi variano a seconda delle terze parti, fare riferimento alla documentazione delle singole terze parti. Ad esempio, gli ambiti di Salesforce sono:

| Valore | Descrizione |
|---|---|
| `api` | Consente di accedere all'account dell'utente connesso in quel momento tramite API come API REST e API in blocco. Questo valore include anche `chatter_api`, che consente l'accesso alle risorse API REST Chatter. |
| `chatter_api` | Consente di accedere solo alle risorse API REST Chatter. |
| `custom_permissions` | Consente di accedere alle autorizzazioni personalizzate di un'organizzazione associate all'applicazione connessa e mostra se per l'utente corrente sono abilitate le singole autorizzazioni. |
| `full` | Consente di accedere a tutti i dati accessibili per l'utente connesso e comprende tutti gli altri ambiti. `full` non restituisce un token di aggiornamento. Per ottenere un token di aggiornamento è necessario richiedere esplicitamente l'ambito `refresh_token`. |
| `id` | Consente l'accesso al servizio URL identità. È possibile richiedere `profile`, `email`, `address` o `phone` singolarmente per ottenere lo stesso risultato che si ottiene con `id`; sono tutti sinonimi. |

EDIZIONI

Disponibile nelle versioni: Lightning Experience e Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:

- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:

- "Personalizza applicazione"

  E

  "Gestisci provider di autenticazione"

| Valore | Descrizione |
|---|---|
| `openid` | Consente l'accesso all'ID univoco dell'utente connesso in quel momento per le Applicazioni connesse OpenID.<br>L'ambito `openid` si può utilizzare nel flusso utente-agente OAuth 2.0 e nel flusso di autenticazione server Web OAuth 2.0 per ottenere un token ID firmato conforme alle specifiche OpenID Connect oltre al token di accesso. |
| `refresh_token` | Consente di restituire un token di aggiornamento se si ha diritto a riceverne uno. Questo permette all'applicazione di interagire con i dati dell'utente mentre questi è offline, ed è sinonimo della richiesta `offline_access`. |
| `visualforce` | Consente di accedere alle pagine Visualforce. |
| `web` | Consente di utilizzare `access_token` sul Web. È incluso anche `visualforce`, che consente di accedere alle pagine Visualforce. |

VEDERE ANCHE:

Uso dei parametri di richiesta con URL di configurazione client

## Uso del parametro Site

Utilizzare il proprio provider di autenticazione per accedere a un sito o collegarsi a un utente del sito.

Per utilizzare il proprio provider con un sito, attenersi a questa procedura:

- Abilitare il provider da utilizzare con un sito
- Assicurarsi che il sito sia configurato per l'utilizzo dello stesso portale
- Aggiungere le informazioni sull'URL di accesso specifico del sito all'URL di configurazione client appropriato, ad esempio l'`URL inizializzazione Single Sign-On`, utilizzando il parametro `site`

Esempio: Quando si crea il sito, si crea la pagina Visualforce di accesso al sito o si specifica la pagina predefinita. Un esempio di URL di accesso al sito è: `https%3A%2F%2Fmysite.force.com%2FSiteLogin`.

Di seguito è riportato un esempio di URL di accesso al sito aggiunto all'`URL inizializzazione Single Sign-On` utilizzando il parametro `site`, dove:

- *`orgID`* è l'ID del provider di autorizzazione
- *`URLsuffix`* è il valore specificato nella definizione del provider di autenticazione

```
https://login.salesforce.com/services/auth/sso/orgID/URLsuffix?site=https%3A%2F%2Fmysite.force.com%2FSiteLogin
```

Se non si specifica un parametro `site`, l'utente viene indirizzato a un portale standard (se impostato per un portale) o all'applicazione standard.

VEDERE ANCHE:

Uso dei parametri di richiesta con URL di configurazione client

EDIZIONI

Disponibile nelle versioni: Lightning Experience e Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:

- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:

- "Personalizza applicazione"

  E

  "Gestisci provider di autenticazione"

## Uso del parametro StartURL

Indirizzare l'utente a una posizione specifica dopo l'autenticazione o il collegamento.

Per indirizzare gli utenti a una posizione specifica dopo l'autenticazione, è necessario specificare un URL con il parametro di richiesta `startURL`. L'URL deve essere un URL relativo; il passaggio di un URL assoluto causa un errore. Se non si aggiunge `startURL`, l'utente viene indirizzato a `/home/home.jsp` (per le applicazioni portale o standard) o alla pagina predefinita del sito (per i siti) al termine dell'autenticazione.

Esempio: Ad esempio, con un `URL inizializzazione Single Sign-On`, l'utente che ha eseguito l'accesso viene indirizzato a questa posizione. Per un `URL di collegamento utente esistente`, il link "Continua in Salesforce" nella pagina di conferma porta a questa pagina.

Di seguito è riportato un esempio di parametro `startURL` aggiunto all'`URL inizializzazione Single Sign-On`, dove:

- *`orgID`* è l'ID del provider di autorizzazione
- *`URLsuffix`* è il valore specificato nella definizione del provider di autenticazione

```
https://login.salesforce.com/services/auth/sso/orgID/URLsuffix?startURL=%2F005x00000000001%3Fnoredirect%3D1
```

VEDERE ANCHE:

Uso dei parametri di richiesta con URL di configurazione client

EDIZIONI

Disponibile nelle versioni: Lightning Experience e Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:

- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:

- "Personalizza applicazione"

  E

  "Gestisci provider di autenticazione"

## Uso del parametro Community negli URL

Per indirizzare l'utente a una comunità specifica dopo l'autenticazione.

Per indirizzare gli utenti a una comunità specifica dopo l'autenticazione, è necessario specificare un URL con il parametro di richiesta `community`. Se non si aggiunge questo parametro, al termine dell'autenticazione l'utente viene indirizzato a `/home/home.jsp` (per le applicazioni portale o standard) o alla pagina predefinita del sito (per i siti).

**Esempio:** Ad esempio, con un `URL inizializzazione Single Sign-On`, l'utente che ha eseguito l'accesso viene indirizzato a questa posizione. Per un `URL di collegamento utente esistente`, il link "Continua in Salesforce" nella pagina di conferma porta a questa pagina.

Di seguito è riportato un esempio di parametro `community` aggiunto all'`URL inizializzazione Single Sign-On`, dove:

- *`orgID`* è l'ID del provider di autenticazione
- *`URLsuffix`* è il valore specificato nella definizione del provider di autenticazione

```
https://login.salesforce.com/services/auth/sso/orgID/URLsuffix?community=https://acme.force.com/support
```

EDIZIONI

Disponibile nelle versioni: Lightning Experience e Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:

- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:

- "Personalizza applicazione"

  E

  "Gestisci provider di autenticazione"

## Utilizzo del parametro Authorization Endpoint

Per inviare gli utenti a un endpoint di autorizzazione specifico.

È possibile aggiungere un parametro `provAuthorizeEndpointHost` all'URL di un provider di autenticazione Salesforce per indirizzare gli utenti a un endpoint di autorizzazione di un dominio prestabilito, ad esempio un dominio personalizzato creato mediante Dominio personale. L'indicazione di un endpoint di autorizzazione consente di usufruire di funzioni come l'individuazione delle sessioni durante l'autorizzazione. Questo parametro è disponibile solo per i provider di autenticazione Salesforce e non si può utilizzare per inviare gli utenti a una pagina di autorizzazione in un dominio esterno a Salesforce.

Per indirizzare gli utenti a un endpoint di autorizzazione Salesforce specifico, è necessario specificare un URL con il parametro di richiesta `provAuthorizeEndpointHost` e un host `https` valido. Le stringhe di query aggiunte alla fine dell'URL dell'host vengono ignorate. È invece possibile specificare un percorso per una comunità.

**Esempio:** Di seguito è riportato un esempio di parametro `provAuthorizeEndpointHost` aggiunto all'URL del provider di autenticazione:

- *`orgID`* è l'ID del provider di autenticazione
- *`URLsuffix`* è il valore specificato nella definizione del provider di autenticazione

```
https://login.salesforce.com/services/auth/sso/orgID/
URLsuffix?provAuthorizeEndpointHost=https%3A%2F%2Fmydomain.my.salesforce.com
```

Di seguito è riportato un esempio di un `provAuthorizeEndpointHost` indirizzato all'URL di una comunità

```
https://login.salesforce.com/services/auth/sso/orgID/
URLsuffix?provAuthorizeEndpointHost=https%3A%2F%2Fmycommunity.force.com%2Fbilling
```

Se non viene indicato un endpoint di autorizzazione, Salesforce utilizza quello predefinito per il provider di autorizzazione. Se per il provider di autorizzazione non esiste un'impostazione predefinita, Salesforce utilizza l'endpoint per login.salesforce.com.

L'endpoint di autorizzazione non modifica l'endpoint del token, che continua a essere l'host configurato o predefinito. Ad esempio, se l'endpoint di autorizzazione è un'istanza di Sandbox e il provider è impostato per utilizzare un endpoint del token di produzione, si verifica un errore nel flusso perché l'autorizzazione è stata concessa solo dall'istanza di Sandbox.

EDIZIONI

Disponibile nelle versioni: Lightning Experience e Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni:

- "Visualizza impostazione e configurazione"

Per modificare le impostazioni:

- "Personalizza applicazione"

  E

  "Gestisci provider di autenticazione"

# Informazioni sui certificati e le chiavi Salesforce

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

AUTORIZZAZIONI UTENTE

Per creare, modificare e gestire certificati:

- "Personalizza applicazione"

Nota: Queste informazioni sono valide per la Crittografia classica e non per la Crittografia piattaforma.

Per utilizzare i certificati e le chiavi di Salesforce, da Imposta immettere *Gestione certificati e chiavi* nella casella Ricerca veloce, quindi selezionare **Gestione certificati e chiavi**. Da questa pagina è possibile gestire:

- I propri certificati
- I certificati di autenticazione
- Le proprie chiavi master di crittografia

## Certificati

I certificati e le coppie di chiavi Salesforce vengono utilizzati per le firme che verificano una richiesta proveniente dall'organizzazione. Vengono usati per le comunicazioni SSL autenticate con un sito Web esterno, oppure quando si utilizza l'organizzazione come provider di identità. È necessario generare una coppia di certificato e chiave Salesforce soltanto se si lavora con un sito Web esterno che richiede la verifica della provenienza di una richiesta da un'organizzazione Salesforce.

Salesforce offre due tipi di certificati:

**Autofirmato**

Un certificato autofirmato è firmato da Salesforce con l'algoritmo SHA-256. Non tutti i siti Web esterni accettano i certificati autofirmati.

**Firmato da una CA**

Un certificato firmato da una CA è firmato da un'autorità di certificazione (CA) esterna. La maggior parte dei siti Web esterni accettano i certificati firmati da una CA. È necessario prima generare la richiesta di firma del certificato da inviare alla CA e quindi importare la versione firmata del certificato prima di poterla utilizzare.

È possibile esportare tutti i certificati e le chiavi private in un archivio delle chiavi per memorizzarli, oppure importare i certificati e le chiavi contenute nell'archivio. Ciò consente di spostare le chiavi da un'organizzazione all'altra. Il file esportato è in formato JKS (Java Keystore) e anche il file importato deve essere in formato JKS. Per ulteriori informazioni sul formato JKS, vedere la documentazione di Java KeyStore di Oracle.

## Certificati di autenticazione reciproca

Nota: Se questa opzione non è visualizzata nella pagina Gestione certificati e chiavi, rivolgersi a Salesforce per abilitare la funzione.

Salesforce può verificare se una richiesta proviene dall'organizzazione utilizzando i certificati Salesforce *e* i certificati tramite connessioni Transport Layer Security (TLS) da client `HTTPS` per l'autenticazione reciproca.

## Chiavi master di crittografia

I campi crittografati con campi personalizzati crittografati, ad esempio i numeri di previdenza sociale o delle carte di credito, utilizzano una chiave master di crittografia per crittografare i dati. Questa chiave viene assegnata automaticamente quando si abilitano i campi

crittografati per la propria organizzazione. È possibile gestire la chiave master in base alle esigenze di protezione della propria organizzazione e ai requisiti di legge.

VEDERE ANCHE:

Creazione di coppie di certificati e chiavi

Caricamento di certificati firmati da un'autorità di certificazione (CA)

Gestione delle chiavi master di crittografia

Modifica di coppie di certificati e chiavi Salesforce

Impostazione dei certificati di autenticazione reciproca

## Creazione di coppie di certificati e chiavi

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

AUTORIZZAZIONI UTENTE

Per creare, modificare e gestire certificati:

- "Personalizza applicazione"

Salesforce offre due tipi di certificati:

**Autofirmato**

Un certificato autofirmato è firmato da Salesforce con l'algoritmo SHA-256. Non tutti i siti Web esterni accettano i certificati autofirmati.

**Firmato da una CA**

Un certificato firmato da una CA è firmato da un'autorità di certificazione (CA) esterna. La maggior parte dei siti Web esterni accettano i certificati firmati da una CA. È necessario prima generare la richiesta di firma del certificato da inviare alla CA e quindi importare la versione firmata del certificato prima di poterla utilizzare.

Per creare un certificato Salesforce:

1. Da Imposta, immettere *Gestione certificati e chiavi* nella casella Ricerca veloce, quindi selezionare **Gestione certificati e chiavi**.
2. Selezionare **Crea certificato autofirmato** o **Crea certificato firmato da una CA**, a seconda del tipo di certificato accettato dal sito Web esterno. Non è possibile modificare il tipo di un certificato dopo averlo creato.
3. Immettere un'etichetta descrittiva per il certificato Salesforce. Questo nome viene utilizzato principalmente dagli amministratori durante la visualizzazione dei certificati.
4. Immettere il Nome univoco. Questo nome viene compilato automaticamente in base all'etichetta del certificato immessa. Il nome può contenere solo caratteri di sottolineatura e alfanumerici e deve essere univoco nell'organizzazione. Deve iniziare con una lettera, non deve includere spazi, terminare con un carattere di sottolineatura, né contenere due caratteri di sottolineatura consecutivi. Utilizzare il Nome univoco per fare riferimento al certificato utilizzando l'API servizi Web Force.com o Apex.
5. Selezionare le Dimensioni chiave per il certificato e le chiavi generate. Per motivi di sicurezza, consigliamo di utilizzare le dimensioni chiave predefinite 2048. Selezionando 2048 si genera un certificato che utilizza chiavi a 2048 bit ed è valido per due anni. Selezionando 1024 si genera un certificato che utilizza chiavi a 1024 bit ed è valido per un anno.

   Nota: Una volta salvato un certificato Salesforce, non è possibile modificare le dimensioni chiave.

6. In caso di creazione di un certificato firmato da una CA, è necessario immettere anche le seguenti informazioni. Questi campi vengono correlati per generare un certificato univoco.

| Campo | Descrizione |
| --- | --- |
| `Nome comune` | Il nome di dominio interamente consentito della società che richiede il certificato firmato. In genere, assume la forma `http://www.miasocietà.com`. |
| `Indirizzo email` | L'indirizzo email associato a questo certificato. |
| `Società` | Il proprio nome sociale o il nome sociale della società. |
| `Reparto` | Ramo della società che utilizza il certificato, ad esempio marketing o contabilità. |
| `Città` | La città nella quale risiede la società. |
| `Stato/Provincia` | Lo stato o la provincia in cui risiede la società. |
| `Codice paese` | Un codice di due lettere che indica il paese nel quale risiede la società. Per gli Stati Uniti, il valore è *`US`*. |

7. Fare clic su **Salva**.

I certificati autofirmati scaricati hanno estensioni `.crt`. Le richieste di firma dei certificati scaricati hanno estensioni `.csr`.

Dopo aver salvato correttamente un certificato Salesforce, il certificato e le chiavi corrispondenti vengono generati automaticamente.

È possibile avere fino a 50 certificati.

Dopo aver creato un certificato firmato da una CA, è necessario caricare il certificato firmato prima di poterlo utilizzare.

Nota: Dopo aver creato un certificato firmato da una CA e una richiesta di certificato, il certificato non è attivo e non può essere utilizzato finché non viene firmato da un'autorità di certificazione e caricato nell'organizzazione.

VEDERE ANCHE:

Informazioni sui certificati e le chiavi Salesforce

Caricamento di certificati firmati da un'autorità di certificazione (CA)

Ripetizione del caricamento di un certificato firmato da una CA

## Caricamento di certificati firmati da un'autorità di certificazione (CA)

Dopo aver creato un certificato firmato da una CA, è necessario effettuare le seguenti operazioni prima che il certificato sia attivo e utilizzabile.

1. Da Imposta, immettere *Gestione certificati e chiavi* nella casella Ricerca veloce, selezionare **Gestione certificati e chiavi**, fare clic sul nome del certificato e quindi su **Scarica richiesta di firma certificato**.
2. Inviare la richiesta di certificato all'autorità di certificazione prescelta.
3. Quando l'autorità di certificazione invia il certificato firmato, da Imposta immettere *Gestione certificati e chiavi* nella casella Ricerca veloce, selezionare **Gestione certificati e chiavi**, fare clic sul nome del certificato e quindi su **Carica certificato firmato**.
4. Fare clic su **Sfoglia** per trovare il certificato firmato da una CA. Il certificato firmato da una CA deve corrispondere a quello creato in Salesforce. Se si tenta di caricare un certificato firmato da una CA diverso, il caricamento non riesce.
5. Fare clic su **Salva** per terminare il caricamento. Fare clic su **Annulla** in qualsiasi momento per non caricare il certificato.

Dopo aver caricato correttamente il certificato firmato, lo stato del certificato viene cambiato in Attivo ed è possibile utilizzare il certificato firmato da una CA.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

AUTORIZZAZIONI UTENTE

Per creare, modificare e gestire certificati:
- "Personalizza applicazione"

Una catena certificati è un ordine gerarchico di certificati nel quale un certificato emette e firma un altro certificato inferiore nella gerarchia. Caricare una catena certificati come singolo certificato firmato da una CA con codifica PEM che rappresenta la catena di certificati concatenati. La catena certificati caricata deve includere i certificati intermedi nell'ordine seguente.

- Iniziare con il certificato server o client e aggiungere il relativo certificato firma.
- In presenza di più certificati intermedi tra il certificato server o client e il certificato principale, aggiungere ogni certificato come certificato che ha firmato il certificato precedente.
- Il certificato principale è facoltativo e in genere non deve essere incluso.

VEDERE ANCHE:

Informazioni sui certificati e le chiavi Salesforce

Ripetizione del caricamento di un certificato firmato da una CA

## Ripetizione del caricamento di un certificato firmato da una CA

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

AUTORIZZAZIONI UTENTE

Per creare, modificare e gestire certificati:

- "Personalizza applicazione"

Se si carica un certificato firmato da una CA e si dimentica di caricare le informazioni complete sul certificato o è necessario caricare un certificato rinnovato, è possibile caricarlo nuovamente per completare l'operazione. In questo modo si risparmia tempo perché non è necessario ricominciare daccapo con una chiave e un certificato nuovi. Quando si ripete il caricamento, i domini dei siti pubblicati vengono ripubblicati automaticamente se hanno almeno un sito o una comunità Force.com. Inoltre, la data di scadenza del record del certificato viene aggiornata con la data di scadenza del certificato appena caricato.

Per caricare nuovamente un certificato firmato da una CA:

1. Da Imposta, immettere *Gestione certificati e chiavi* nella casella Ricerca veloce, quindi selezionare **Gestione certificati e chiavi**.
2. Fare clic sul nome del certificato firmato da una CA da caricare nuovamente.

   Nota: Il certificato dovrebbe avere un'estensione .crt.

3. Fare clic su **Aggiorna certificato firmato** e su **Scegli file**.
4. Fare clic su **Sfoglia** per trovare il certificato firmato da una CA. La chiave pubblica del certificato firmato da una CA deve corrispondere alla chiave pubblica del record del certificato creato in Salesforce. Se si tenta di caricare un certificato firmato da una CA diverso, il caricamento non riesce.

   Nota: Facendo clic su **Annulla** è possibile annullare il caricamento in qualsiasi momento.

5. Fare clic su **Salva** per terminare il caricamento.

Una catena certificati è un ordine gerarchico di certificati nel quale un certificato emette e firma un altro certificato inferiore nella gerarchia. Caricare una catena certificati come singolo certificato firmato da una CA con codifica PEM che rappresenta la catena di certificati concatenati. La catena certificati caricata deve includere i certificati intermedi nell'ordine seguente.

- Iniziare con il certificato server o client e aggiungere il relativo certificato firma.
- In presenza di più certificati intermedi tra il certificato server o client e il certificato principale, aggiungere ogni certificato come certificato che ha firmato il certificato precedente.
- Il certificato principale è facoltativo e in genere non deve essere incluso.

VEDERE ANCHE:

Informazioni sui certificati e le chiavi Salesforce

Caricamento di certificati firmati da un'autorità di certificazione (CA)

## Impostazione dei certificati di autenticazione reciproca

Utilizzare l'autenticazione reciproca per l'organizzazione creando un certificato di autenticazione reciproca.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Personal Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per creare, modificare e gestire certificati:
- "Personalizza applicazione"

> Nota: Se questa opzione non è visualizzata nella pagina Gestione certificati e chiavi, rivolgersi a Salesforce per abilitare la funzione.

Attenersi alla procedura che segue per caricare un certificato.

1. Fare clic su **Carica certificato di autenticazione reciproca**.
2. Assegnare al certificato un'etichetta e un nome e fare clic su **Scegli file** per individuare il certificato.
3. Fare clic su **Salva** per terminare il caricamento.
4. Abilitare l'autorizzazione utente "Imponi autenticazione reciproca SSL/TLS" per un utente "Solo API". Questo utente "Solo API" configura il client API per connettersi alla porta 8443 e presentare il certificato del client firmato.

Tenere presente che quando si contatta la porta 8443 il certificato client deve includere gli eventuali certificati intermedi nella catena dei certificati.

Una catena certificati è un ordine gerarchico di certificati nel quale un certificato emette e firma un altro certificato inferiore nella gerarchia. Caricare una catena certificati come singolo certificato firmato da una CA con codifica PEM che rappresenta la catena di certificati concatenati. La catena certificati caricata deve includere i certificati intermedi nell'ordine seguente.

- Iniziare con il certificato server o client e aggiungere il relativo certificato firma.
- In presenza di più certificati intermedi tra il certificato server o client e il certificato principale, aggiungere ogni certificato come certificato che ha firmato il certificato precedente.
- Il certificato principale è facoltativo e in genere non deve essere incluso.

VEDERE ANCHE:

Informazioni sui certificati e le chiavi Salesforce

Configurazione del client API per l'uso dell'autenticazione reciproca

## Configurazione del client API per l'uso dell'autenticazione reciproca

Imporre l'autenticazione reciproca SSL/TLS.

Prima di configurare il client API, è necessario aver completato la procedura di Impostazione dei certificati di autenticazione reciproca.

1. Accedere al servizio Salesforce utilizzando la porta 8443. Includere:
   a. Le proprie credenziali
   b. Le informazioni sul certificato firmato

   Ad esempio, la configurazione che utilizza `cURL` potrebbe avere questo aspetto, dove "@login.txt" contiene il messaggio Soap di accesso con le credenziali dell'utente e "fullcert.pem:xxxxxx" rappresenta le informazioni sul certificato:

```
curl -k https://na1.salesforce.com:8443/services/Soap/u/31.0 -H "Content-Type: text/xml;
 charset=UTF-8" -H "SOAPAction: login" -d @login.txt -v -E fullcert.pem:xxxxxx
```

2. Dopo che la chiamata restituisce un ID sessione, è possibile eseguire altre azioni, ad esempio le query. Ad esempio:

```
curl -k https://na1.salesforce.com:8443/services/Soap/u/31.0 -H "Content-Type: text/xml;
 charset=UTF-8" -H "SOAPAction: example" -d @accountQuery.xml -v -E fullcert.pem:xxxxxx
```

   dove @accountQuery.xml è il nome del file contenente il messaggio Soap di query con l'ID sessione della risposta di accesso.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Personal Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per creare, modificare e gestire certificati:
- “Personalizza applicazione”

Per imporre l'autenticazione reciproca sulla porta 8443 per le connessioni SSL/TLS standard:

(Assegnare a utenti con l'autorizzazione utente "Solo API".)
- "Imponi autenticazione reciproca SSL/TLS"

Per accedere a Salesforce solo mediante un'API Salesforce:
- "Utente solo API"

VEDERE ANCHE:

Informazioni sui certificati e le chiavi Salesforce

Impostazione dei certificati di autenticazione reciproca

## Gestione delle chiavi master di crittografia

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

AUTORIZZAZIONI UTENTE

Per creare, modificare e gestire certificati:

- "Personalizza applicazione"

Nota: Queste informazioni sono valide per la Crittografia classica e non per la Crittografia piattaforma.

I campi crittografati con campi personalizzati crittografati, ad esempio i numeri di previdenza sociale o delle carte di credito, utilizzano una chiave master di crittografia per crittografare i dati. Questa chiave viene assegnata automaticamente quando si abilitano i campi crittografati per la propria organizzazione. È possibile gestire la chiave master in base alle esigenze di protezione della propria organizzazione e ai requisiti di legge. Con le chiavi master di crittografia è possibile effettuare le operazioni seguenti:

- Archiviare la chiave esistente e crearne una nuova
- Esportare una chiave esistente dopo averla archiviata
- Eliminare una chiave esistente
- Importare una chiave esistente dopo averla eliminata

### Archiviazione e creazione di nuove chiavi

Per archiviare la chiave corrente e crearne una nuova:

1. Da Imposta, immettere *Gestione certificati e chiavi* nella casella `Ricerca veloce`, quindi selezionare **Gestione certificati e chiavi**.
2. Fare clic su **Archivia chiave corrente e crea nuova chiave**.
3. Viene visualizzato un messaggio di avviso che informa che si stanno modificando le chiavi. Fare clic su **OK**.
4. La nuova chiave viene generata, le viene assegnato il numero sequenziale successivo e quindi viene attivata.

Tutti i nuovi dati vengono crittografati utilizzando la nuova chiave. I dati esistenti continuano a utilizzare la chiave archiviata finché non vengono modificati e salvati. Quindi, i dati vengono crittografati utilizzando la nuova chiave.

Dopo aver archiviato una chiave, è possibile esportarla o eliminarla.

### Esportazione delle chiavi

È possibile esportare le chiavi in una posizione di backup per conservarle in modo sicuro. È consigliabile esportare una copia di ciascuna chiave prima di eliminarla.

L'esportazione genera un file di testo con la chiave crittografata. È possibile reimportare la chiave nella propria organizzazione in un momento successivo.

Fare clic su `Esporta` accanto alla chiave che si desidera esportare.

### Eliminazione delle chiavi

Non eliminare una chiave a meno che non si sia assolutamente sicuri che non vi siano dati attualmente crittografati con quella chiave. Una volta eliminata una chiave, non è più possibile accedere ai dati crittografati con quella chiave. Se si esporta la chiave prima di eliminarla, è possibile reimportarla nella propria organizzazione.

Per eliminare una chiave, fare clic su `Elimina` accanto alla chiave da eliminare.

Viene visualizzata la data di eliminazione della chiave.

### Importazione delle chiavi

Se si hanno dati associati a una chiave eliminata, è possibile reimportare una chiave esportata nella propria organizzazione. I dati non accessibili diventano nuovamente accessibili.

Fare clic su `Importa` accanto alla chiave che si desidera importare.

VEDERE ANCHE:

Informazioni sui certificati e le chiavi Salesforce

## Modifica di coppie di certificati e chiavi Salesforce

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

AUTORIZZAZIONI UTENTE

Per creare, modificare e gestire certificati:

- "Personalizza applicazione"

Dopo aver creato un certificato Salesforce (inclusi, se abilitati, i certificati di autenticazione reciproca), è possibile modificare soltanto l'`Etichetta` e il `Nome univoco`. Non è possibile modificare elementi come tipo, dimensioni chiave o altre proprietà. Il certificato e le chiavi non vengono generati nuovamente quando si modifica un certificato Salesforce.

Avvertenza: Apex e l'API Servizi Web Force.com utilizzano il `Nome univoco` per accedere al certificato. La modifica del `Nome univoco` potrebbe provocare il danneggiamento del codice.

Per modificare un certificato Salesforce:

1. Da Imposta, immettere *`Gestione certificati e chiavi`* nella casella `Ricerca veloce`, quindi selezionare **Gestione certificati e chiavi**.
2. Fare clic su **Modifica** accanto al nome di un certificato Salesforce.
3. Apportare le modifiche e fare clic su **Salva**.

Per eliminare un certificato, fare clic su **Canc**. Se un certificato viene usato nell'ambito della configurazione del proprio provider di identità, non è possibile eliminarlo.

VEDERE ANCHE:

Informazioni sui certificati e le chiavi Salesforce

## Visualizzazione delle coppie di certificati e chiavi Salesforce

Per visualizzare i dettagli di un certificato Salesforce, da Imposta immettere `Gestione certificati e chiavi` nella casella `Ricerca veloce`, selezionare **Gestione certificati e chiavi** e quindi fare clic sul nome di un certificato.

Dalla pagina dei dettagli del certificato, è possibile effettuare una delle operazioni seguenti:

- Fare clic su **Modifica** per modificare l'etichetta o il nome univoco del certificato.
- Fare clic su **Elimina** per eliminare il certificato.
- Fare clic su **Scarica certificati** per scaricare il certificato completo codificato base64. Questa opzione è disponibile soltanto per i certificati attivi. Per i certificati firmati da una CA, è necessario caricare il certificato firmato prima di poterlo scaricare o utilizzare.
- Fare clic su **Scarica richiesta di firma certificato** per i certificati firmati da una CA per i quali non è ancora stato caricato il certificato firmato.
- Fare clic su **Carica certificato firmato** per caricare il certificato firmato da una CA o per caricarlo una seconda volta.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

AUTORIZZAZIONI UTENTE

Per creare, modificare e gestire certificati:
- "Personalizza applicazione"

VEDERE ANCHE:

Informazioni sui certificati e le chiavi Salesforce
Impostazione dei certificati di autenticazione reciproca

# Informazioni sui provider di identità e i fornitori di servizi

Un *provider di identità* è un provider attendibile che consente di utilizzare il Single Sign-On per accedere ad altri siti Web. Un *fornitore di servizi* è un sito Web che ospita delle applicazioni. È possibile abilitare Salesforce come provider di identità, quindi definire uno o più fornitori di servizi in modo che gli utenti possano accedere ad altre applicazioni direttamente da Salesforce utilizzando il Single Sign-On. Ciò può rivelarsi molto utile per gli utenti, che, anziché dover ricordare molte password, dovranno ricordarne solo una. Inoltre, le applicazioni possono essere aggiunte sotto forma di schede all'organizzazione Salesforce, perciò gli utenti non dovranno più passare da un programma all'altro.

Prima di poter abilitare Salesforce come provider di identità, è necessario impostare un dominio.

L'abilitazione di Salesforce come provider di identità richiede un certificato Salesforce e una coppia di chiavi firmati da un'autorità di certificazione esterna (CA) o autofirmati. Se non è stata generata una coppia di certificato e chiave Salesforce, quando si abilita Salesforce come provider di identità ne viene generata automaticamente una. È anche possibile selezionare un certificato creato in precedenza oppure creare il proprio.

Salesforce utilizza lo standard SAML 2.0 per il Single Sign-On e genera asserzioni SAML quando viene configurato come provider di identità.

Utilizzare il registro eventi del provider di identità se gli utenti rilevano degli errori quando tentano di accedere alle applicazioni del fornitore di servizi.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Developer Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Definire e modificare i provider di identità e i fornitori di servizi:
- "Personalizza applicazione"

## Utilizzo dei provider di identità e dei fornitori di servizi

Salesforce supporta:

- Accesso avviato dal provider di identità: quando Salesforce accede a un fornitore di servizi su iniziativa dell'utente finale.

- Accesso avviato dal fornitore di servizi: quando il fornitore di servizi richiede a Salesforce di autenticare un utente, su iniziativa dell'utente finale.

Di seguito è descritto il flusso generale quando Salesforce effettua l'accesso a un fornitore di servizi come provider di identità.



1. L'utente tenta di accedere a un fornitore di servizi già definito in Salesforce.
2. Salesforce invia una risposta SAML al fornitore di servizi.
3. Il fornitore di servizi identifica l'utente e autentica il certificato.
4. Se l'utente è identificato, viene effettuato l'accesso al fornitore di servizi.

Di seguito viene riportato il flusso generale quando un fornitore di servizi avvia l'accesso e utilizza Salesforce per identificare l'utente.

Service Provider

Salesforce.com as Identity Provider

Requests secure session

Identifies the user

Authenticates certificate if available

Sends response

Authenticates certificate or metadata

Enables login

1. Il fornitore di servizi invia una richiesta SAML valida. L'endpoint viene generato automaticamente quando viene definito il fornitore di servizi: si tratta dell'`SP-Initiated POST Endpoint`.
2. Salesforce identifica l'utente incluso nella richiesta SAML.

```
<samlp:AuthnRequest ID="bndkmeemcaamihajeloilkagfdliilbhjjnmlmfo" Version="2.0"
   IssueInstant="2010-05-24T22:57:19Z"
   ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
   ProviderName="google.com" IsPassive="false"
   AssertionConsumerServiceURL="https://www.google.com/a/resp.info/acs">
   <saml:Issuer>google.com</saml:Issuer>
   <samlp:NameIDPolicy AllowCreate="true"
   Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"/>
</samlp:AuthnRequest>
```

   Se all'interno della definizione è stato incluso un certificato, Salesforce autentica il certificato.

   Nota: se nella definizione del fornitore di servizi è incluso un certificato e la richiesta SAML non ne contiene uno, la richiesta ha esito negativo e l'utente non può accedere utilizzando Salesforce. Se la definizione non include un certificato e la richiesta include una firma, la richiesta ha esito positivo se l'utente viene identificato correttamente.

3. Se l'utente non ha ancora effettuato l'accesso a Salesforce, viene invitato ad accedere.

4. Salesforce invia una risposta SAML al fornitore di servizi.
5. Il fornitore di servizi autentica la risposta SAML inviata da Salesforce. Se l'utente è stato autenticato, viene effettuato l'accesso al fornitore di servizi. L'utente accede anche a Salesforce.

   **Importante:** Salesforce non dispone di alcun meccanismo per disconnettere automaticamente l'utente da Salesforce quando l'utente si disconnette dal fornitore di servizi.

Di seguito è riportato un esempio della risposta SAML da Salesforce. È possibile condividere queste informazioni con il proprio fornitore di servizi.


```
<samlp:Response Destination="https://login-blitz03.soma.salesforce.com/
?saml=MgoTx78aEPa2r1BHKCHmlfUKhH2mkDrXOjmYcjHG_qNDbsRM_6ZAo.wvGk"
  ID="_0f551f9288c8b76f21c3d4d15c9cd1df1290476801091"
  InResponseTo="_2INwHuINDJTvjo8ohcM.Fpw_uLukYi0WArVx2IJD569kZYL
    osBwuiaSbzzxOPQjDtfw52tJB10VfgPW2p5g7Nlv5k1QDzR0EJYGgn0d0z8
    CIiUOY31YBdk7gwEkTygiK_lb46IO1fzBFoaRTzwvf1JN4qnkGttw3J6L4b
    opRI8hSQmCumM_Cvn3DHZVN.KtrzzOAflcMFSCY.bj1wvruSGQCooTRSSQ"
  IssueInstant="2010-11-23T01:46:41.091Z" Version="2.0">
<saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
>identityorg.blitz03.blitz.salesforce.com</saml:Issuer>
–
<ds:Signature>
–
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
–
<ds:Reference URI="#_0f551f9288c8b76f21c3d4d15c9cd1df1290476801091">
–
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
–
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<ec:InclusiveNamespaces PrefixList="ds saml samlp xs"/>
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>4NVTbQ2WavD+ZBiyQ7ufc8EhtZw=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
–
<ds:SignatureValue>

eqrkFxNlJRCT4VQ7tt7wKZGK7oLCCCa4gV/HNcL03RoKbSXIcwU2CAqW0qTSj25FqhRe2fOwAYa5
xFWat7Fw2bbncU+/nnuVNZut8HEEQoHiQA/Jrh7XB4CNlOpM1QRvgB5Dtdkj/0lI4h3X3TFix57B
sgZJGbb5PWEqSH3ZAl+NPvW9nNtYQIFyCTe9+cw2BhCxFgSWfP3/kIYHSM2gbIy27CrRrFS1lAqP
hKSLaH+ntH1E09gp78RSyJ2WKFGJU22sE9RJSZwdVw3VGG06Z6RpSjPJtaREELhhIBWTHNoF+VvJ
2Hbexjew6CO08lXRDe8dbrrPIRK/qzHZYf1H0g==
</ds:SignatureValue>
–
<ds:KeyInfo>
–
<ds:X509Data>
```

```
–
<ds:X509Certificate>
MIIEbjCCA1agAwIBAgIOASh04QulAAAAAClXs7MwDQYJKoZIhvcNAQEFBQAwfTEVMBMGA1UEAwwM
SWRlbnRpdHkgT3JnMRgwFgYDVQQLDA8wMEREMDAwMDAwMEZIOGwxFzAVBgNVBAoMDlNhbGVzZm9y
Y2UuY29tMRYwFAYDVQQHDA1TYW4gRnJhbmNpc2NvMQswCQYDVQQIDAJDQTEMMAoGA1UEBhMDVVNB
MB4XDTEwMDUwNzIyMjcwNVoXDTEyMDUwNjIyMjcwNVowfTEVMBMGA1UEAwwMSWRlbnRpdHkgT3Jn
MRgwFgYDVQQLDA8wMEREMDAwMDAwMEZIOGwxFzAVBgNVBAoMDlNhbGVzZm9yY2UuY29tMRYwFAYD
VQQHDA1TYW4gRnJhbmNpc2NvMQswCQYDVQQIDAJDQTEMMAoGA1UEBhMDVVNBMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyM4/sjoaizbnWTDjt9mGht2fDGxnLCWGMJ+D+9NWXD5wM15N
SFEcflpI9W4makcCGvoac+CVbPTmOUzOsCQzu7iGkLeMMpngf2XqllnJgl4ejuH8socNrDtltaMk
hC08KAmli3Wm/okllqSjVOl8H52jtbvm6HkvLVj2NDLRY6kUejVZMGjGwV5E0FJliwgIip4sCchl
dkahbNjbikiiv1MAs8xHbtBt3wnKZWJq3JtS0va1sazUVmEwGDlVW43QPF0S7eV3IJFFhyCPV8yF
N3k0wCkCVBWoknwkMA8CbD+p6qNBVmvh3F3IaW2oym/1eSvtMLNtrPJeZzssqDYqgQIDAQABo4Hr
MIHoMB0GA1UdDgQWBBTYSVEZ9r8Q8T2rbZxPFfPYPZKWITCBtQYDVR0jBIGtMIGqgBTYSVEZ9r8Q
8T2rbZxPFfPYPZKWIaGBgaR/MH0xFTATBgNVBAMMDElkZW50aXR5IE9yZzEYMBYGA1UECwwPMDBE
RDAwMDAwMDBGSDhsMRcwFQYDVQQKDA5TYWxlc2ZvcmNlLmNvbTEWMBQGA1UEBwwNU2FuIEZyYW5j
aXNjbzELMAkGA1UECAwCQ0ExDDAKBgNVBAYTA1VTQYIOASh04QupAAAAAClXs7MwDwYDVR0TAQH/
BAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEANaO5Tqcc56E6Jv8itwjtbPvR+WHEMnZgQ9cCPF5Q
VACd5v7I/srx4ZJt/ZO4RZkmX1FXla0M7JGOu63eELHYG1DxT1SpGmpOL7xfBn7QUoh8Rmpp3BZC
WCPIcVQHLs1LushsrpbWu+85tgzlVN4sFVBl8F9rohhbM1dMOUAksoQgM3avcZ2vkugKhX40vIuf
Gw4wXZe4TBCfQay+eDONYhYnmlxVV+dJyHheENOYfVqlau8RMNhRNmhXlGxXNQyU3kpMaTxOux8F
DyOjc5YPoe6PYQ0C/mC77ipnjJAjwm+Gw+heK/9NQ7fIonDObbfu2rOmudtcKG74IDwkZL8HjA==
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
–
<samlp:Status>
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
</samlp:Status>
–
<saml:Assertion ID="_e700bf9b25a5aebdb9495fe40332ef081290476801092"
IssueInstant="2010-11-23T01:46:41.092Z" Version="2.0">
<saml:Issuer
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">identityorg.blitz03.blitz.salesforce.com</saml:Issuer>
–
<saml:Subject>
<saml:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">charliemortimore@gmail.com</saml:NameID>
–
<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData NotOnOrAfter="2010-11-23T01:51:41.093Z"
Recipient="https://login-blitz03.soma.salesforce.com/?saml=MgoTx78aEPa2r1BHKCHmlfUKhH2mkDrXOjmYcjHG_qNDbsRM_6ZAo.wvGk"/>
</saml:SubjectConfirmation>
</saml:Subject>
–
<saml:Conditions NotBefore="2010-11-23T01:46:41.093Z"
NotOnOrAfter="2010-11-23T01:51:41.093Z">
–
<saml:AudienceRestriction>
<saml:Audience>https://childorgb.blitz03.blitz.salesforce.com</saml:Audience>
</saml:AudienceRestriction>
</saml:Conditions>
```

```
–
<saml:AuthnStatement AuthnInstant="2010-11-23T01:46:41.092Z">
–
<saml:AuthnContext>
<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</saml:AuthnContextClassRef>
</saml:AuthnContext>
</saml:AuthnStatement>
–
<saml:AttributeStatement>
–
<saml:Attribute Name="userId"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml:AttributeValue xsi:type="xs:anyType">005D0000001Ayzh</saml:AttributeValue>
</saml:Attribute>
–
<saml:Attribute Name="username"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml:AttributeValue xsi:type="xs:anyType">admin@identity.org</saml:AttributeValue>
</saml:Attribute>
–
<saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml:AttributeValue xsi:type="xs:anyType">cmortimore@salesforce.com</saml:AttributeValue>
</saml:Attribute>
–
<saml:Attribute Name="is_portal_user"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml:AttributeValue xsi:type="xs:anyType">false</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>
```


VEDERE ANCHE:


- Abilitazione di Salesforce come provider di identità
- Visualizzazione dei dettagli del provider di identità
- Prerequisiti per la definizione dei fornitori di servizi
- Definizione dei fornitori di servizi come applicazioni connesse con abilitazione SAML
- Mappatura degli utenti di Salesforce agli utenti delle applicazioni
- Visualizzazione dei dettagli del fornitore di servizi
- Abilitazione dei provider di identità e definizione dei fornitori di servizi per i portali e i siti
- Esempi di utilizzo dei provider di identità e dei fornitori di servizi

## Abilitazione di Salesforce come provider di identità

Per abilitare Salesforce come provider di identità:

1. Impostare un dominio utilizzando Dominio personale e distribuirlo a tutti gli utenti.
2. Da Imposta, immettere *Provider di identità* nella casella `Ricerca veloce`, selezionare **Provider di identità** e fare clic su **Abilita Provider di identità**.
3. Per impostazione predefinita, un provider di identità Salesforce utilizza un certificato autofirmato generato automaticamente con l'algoritmo di firma SHA-256. Se sono già stati creati certificati autofirmati, selezionare il certificato da utilizzare quando si comunica in modo protetto con altri servizi.

   Se si desidera utilizzare un certificato firmato da una CA anziché un certificato autofirmato, seguire questa procedura.

   a. Creare e importare un nuovo certificato firmato da una CA. Per le istruzioni, vedere Informazioni sui certificati e le chiavi Salesforce.
   b. Da Imposta, immettere *Provider di identità* nella casella `Ricerca veloce`, quindi selezionare **Provider di identità**.
   c. Fare clic su **Modifica** e selezionare il certificato firmato da una CA.
   d. Fare clic su **Salva**.

Dopo aver abilitato Salesforce come provider di identità, è possibile definire i fornitori di servizi creando applicazioni connesse (da Imposta, immettere *Applicazioni* nella casella `Ricerca veloce`, quindi selezionare **Applicazioni**).

VEDERE ANCHE:

Informazioni sui provider di identità e i fornitori di servizi
Creazione di coppie di certificati e chiavi

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Developer Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Definire e modificare i provider di identità e i fornitori di servizi:

- "Personalizza applicazione"

## Visualizzazione dei dettagli del provider di identità

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Developer Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Definire e modificare i provider di identità e i fornitori di servizi:

- "Personalizza applicazione"

Dopo aver abilitato un provider di identità per l'organizzazione, è possibile visualizzare i dettagli da Imposta immettendo `Provider di identità` nella casella `Ricerca veloce` e selezionando **Provider di identità**. È possibile condividere queste informazioni, ad esempio l'`Emittente`, con il proprio fornitore di servizi.

Da questa pagina è possibile fare clic su:

- **Modifica** per modificare il certificato associato al provider di identità.

  Avvertenza: La modifica del certificato può disabilitare l'accesso alle applicazioni esterne. Potrebbe essere necessario aggiornare tutte le applicazioni esterne per convalidare le informazioni sul nuovo certificato.

- **Disabilita** per disabilitare il provider di identità.

  Avvertenza: se si disabilita il provider di identità, gli utenti non potranno più accedere alle applicazioni esterne.

- **Scarica certificati** per scaricare il certificato associato al provider di identità. Il fornitore di servizi può utilizzare queste informazioni per connettersi a Salesforce.
- **Scarica metadati** per scaricare i metadati associati al provider di identità. Il fornitore di servizi può utilizzare queste informazioni per connettersi a Salesforce.
- Nella sezione Endpoint Discovery metadati SAML è possibile accedere agli URL relativi alle informazioni del provider di identità SAML per il dominio personalizzato e per ciascuna comunità. Il fornitore di servizi può utilizzare tali URL per configurare il Single Sign-On per la connessione a Salesforce.
  - Salesforce Identity: URL dei metadati del provider di identità per il dominio personalizzato in Dominio personale.
  - `Nome comunità` Community Identity: URL dei metadati del provider di identità per la comunità denominata.
- Nella sezione dei fornitori di servizi, accanto al nome di un fornitore di servizi già definito, fare clic su **Modifica** per modificarne la definizione, su **Profili** per aggiungere o eliminare i profili utente che hanno accesso a questo fornitore di servizi oppure su **Canc** per eliminarlo.

  Nota: per definire un nuovo fornitore di servizi, da Imposta, immettere `Applicazioni` nella casella `Ricerca veloce`, quindi selezionare **Applicazioni** e creare una nuova applicazione connessa con abilitazione SAML.

VEDERE ANCHE:

Informazioni sui provider di identità e i fornitori di servizi

## Prerequisiti per la definizione dei fornitori di servizi

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Developer Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Definire e modificare i provider di identità e i fornitori di servizi:
- "Personalizza applicazione"

Prima di definire un fornitore di servizi:

1. Abilitare Salesforce come provider di identità.
2. Dare al fornitore di servizi informazioni sulla configurazione di Salesforce come provider di identità. Queste informazioni sono disponibili come metadati che possono essere scaricati e trasmessi al fornitore di servizi per una semplice configurazione. Tuttavia, non tutti i fornitori di servizi supportano i metadati. Se il fornitore di servizi utilizzato supporta i certificati, potrebbe essere necessario scaricare il certificato. Da Imposta, immettere *`Provider di identità`* nella casella `Ricerca veloce`, selezionare **Provider di identità** e fare clic su **Scarica certificati** o su **Scarica metadati**.
3. Chiedere al fornitore di servizi le seguenti informazioni:
   - URL del servizio consumatori dell'asserzione (ACS)
   - ID entità
   - Tipo di oggetto: specifica se l'oggetto della risposta SAML da Salesforce (come provider di identità) è un nome utente Salesforce o un ID federazione
   - Certificato di protezione: necessario solo quando il fornitore di servizi avvia l'accesso a Salesforce e firma le richieste SAML

VEDERE ANCHE:

Informazioni sui provider di identità e i fornitori di servizi

## Definizione dei fornitori di servizi come applicazioni connesse con abilitazione SAML

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Developer Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Definire e modificare i provider di identità e i fornitori di servizi:
- "Personalizza applicazione"

1. Completare i prerequisiti.
2. Da Imposta, immettere *`Applicazioni`* nella casella `Ricerca veloce`, quindi selezionare **Applicazioni**.
3. In Applicazione connessa, fare clic su **Nuova**.
4. Specificare i campi obbligatori in Informazioni di base.
5. In Impostazioni app Web, selezionare **Abilita SAML** e indicare i seguenti valori:

   **ID entità**

   Questo valore proviene dal fornitore di servizi. Ogni ID entità dell'organizzazione deve essere univoco. Se si accede a più applicazioni del fornitore di servizi, è sufficiente definire il fornitore una sola volta, e quindi utilizzare il parametro `RelayState` per aggiungere i valori dell'URL e indirizzare l'utente all'applicazione richiesta dopo che ha eseguito l'accesso.

   **URL ACS**

   L'URL ACS, o Assertion Consumer Service, è fornito dal fornitore di servizi SAML.

   **Tipo di oggetto**

   Specifica il campo che definisce l'identità dell'utente per l'applicazione. Le opzioni possibili sono il nome utente, l'ID federazione, l'ID utente, un attributo personalizzato o un ID persistente calcolato mediante algoritmo. Un attributo personalizzato può essere qualsiasi campo personalizzato aggiunto all'oggetto Utente nell'organizzazione, purché sia uno dei seguenti tipi di dati: Email, Testo, URL o Formula (con tipo di testo restituito). Quando si

seleziona `Attributo personalizzato` come **Tipo di oggetto**, Salesforce visualizza un campo **Attributo personalizzato** con un elenco dei campi personalizzati disponibili per l'oggetto Utente nell'organizzazione.

**Formato ID nome**

Specifica il l'attributo del formato inviato nei messaggi SAML. Per impostazione predefinita è selezionato "Non specificato". A seconda del fornitore di servizi SAML, può essere opportuno impostare questa opzione su indirizzo email, persistente o temporaneo.

**Emittente**

Per impostazione predefinita viene utilizzato l'emittente standard per il provider di identità (il Dominio personale dell'organizzazione). Se il fornitore di servizi SAML richiede un valore diverso, specificarlo in questo campo.

6. L'indicazione dei valori seguenti è facoltativa:

**URL iniziale**

Indirizza gli utenti a una pagina specifica quando eseguono l'applicazione. L'URL iniziale può essere un URL assoluto, ad esempio `https://na1.salesforce.com/001/o`, o può essere il link al nome dell'applicazione, ad esempio `https://customer.goodApp.com` per GoodApp. Se si indica un URL iniziale si rende disponibile l'applicazione nel menu delle applicazioni Force.com e nel Programma di avvio applicazione.

**Verifica firme per le richieste**

Selezionare `Verifica firme per le richieste` se il provider di servizi ha messo a disposizione un certificato di protezione. Cercare il certificato nel sistema. Questa operazione è necessaria solo se si intende avviare l'accesso a Salesforce dal fornitore di servizi e se il fornitore di servizi firma le richieste SAML.

Importante: se si carica un certificato, tutte le richieste SAML devono essere firmate. Se non viene caricato un certificato, vengono accettate tutte le richieste SAML.

**Crittografa risposta SAML**

Selezionare `Crittografa risposta SAML` per caricare un certificato e selezionare un metodo per crittografare l'asserzione. I valori validi per l'algoritmo di crittografia sono `AES–128` (chiave a 128 bit), `AES–256` (chiave a 256 bit) e `Triple DES` (Triple Data Encryption Algorithm).

7. Fare clic su **Salva**.

Per autorizzare gli utenti per questa applicazione SAML:

1. Da Imposta, immettere *`Applicazioni connesse`* nella casella `Ricerca veloce`, quindi selezionare l'opzione di gestione delle applicazioni connesse.
2. Fare clic sul nome dell'applicazione.
3. Selezionare i profili e/o gli insiemi di autorizzazioni che possono accedere all'applicazione.

VEDERE ANCHE:

Informazioni sui provider di identità e i fornitori di servizi

## Mappatura degli utenti di Salesforce agli utenti delle applicazioni

Se il `Tipo di oggetto` per la definizione del fornitore di servizi è `ID federazione`, è necessario mappare l'utente Salesforce al nome utente utilizzato per accedere al fornitore di servizi.

Per mappare l'utente Salesforce all'utente dell'applicazione:

1. Da Imposta, immettere *Utenti* nella casella `Ricerca veloce`, selezionare **Utenti**, quindi fare clic su **Modifica** per ogni utente da mappare.
2. In `ID federazione`, nella sezione Informazioni su Single Sign On, immettere il nome utente da utilizzare per accedere al fornitore di servizi.
3. Fare clic su **Salva**.

Suggerimento: Utilizzare l'API SOAP se si devono aggiornare grandi quantità di profili utente o insiemi di autorizzazioni. Vedere il manuale *SOAP API Developer's Guide*.

VEDERE ANCHE:

Informazioni sui provider di identità e i fornitori di servizi

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Developer Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Definire e modificare i provider di identità e i fornitori di servizi:

- "Personalizza applicazione"

## Visualizzazione dei dettagli del fornitore di servizi

Dopo che si è definito un fornitore di servizi per la propria organizzazione mediante la creazione di un'applicazione connessa con abilitazione SAML è possibile visualizzarne i dettagli da Imposta immettendo *Applicazioni connesse* nella casella `Ricerca veloce`, selezionando **Applicazioni connesse** e quindi il nome dell'applicazione. Potrebbe essere necessario condividere queste informazioni, quali `SP-Initiated POST Endpoint` o `SP-Initiated Redirect Endpoint`, con i fornitori di servizi.

Da questa pagina è possibile fare clic su:

- **Modifica** per cambiare i valori della definizione del fornitore di servizi.
- **Elimina** per eliminare una definizione di fornitore di servizi.

  Avvertenza: se si elimina una definizione del fornitore di servizi, gli utenti non avranno più accesso a quel fornitore di servizi.

- **Accesso profilo** per cambiare i profili che hanno accesso a questo fornitore di servizi.

VEDERE ANCHE:

Informazioni sui provider di identità e i fornitori di servizi

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Developer Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Definire e modificare i provider di identità e i fornitori di servizi:

- "Personalizza applicazione"

## Abilitazione dei provider di identità e definizione dei fornitori di servizi per i portali e i siti

Durante l'abilitazione dei provider di identità e la definizione dei fornitori di servizi per i siti Force.com, i Portali Clienti e i portali partner, tenere presente quanto segue:

- Durante la definizione di un fornitore di servizi, se il `Tipo di oggetto` è `Nome utente`, l'ID dell'organizzazione Salesforce viene inserito davanti al nome utente nell'asserzione SAML. Ad esempio, se l'utente è `mRossi@WFC.com`, l'oggetto dell'asserzione SAML contiene `00DE0000000FFLT@mRossi@WFC.com`. Se il `Tipo di oggetto` è `ID federazione`, viene utilizzato l'ID federazione esatto.
- L'attributo `is_portal_user` incluso nell'asserzione SAML generata da Salesforce contiene dei valori. È possibile condividere il seguente esempio con il proprio fornitore di servizi.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Developer Edition**, **Enterprise Edition**, **Performance Edition** e **Unlimited Edition**

AUTORIZZAZIONI UTENTE

Definire e modificare i provider di identità e i fornitori di servizi:

- "Personalizza applicazione"

```
<saml:Attribute Name="is_portal_user"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue
         xmlns:xs="http://www.w3.org/2001/XMLSchema"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:type="xs:anyType">true
      </saml:AttributeValue>
</saml:Attribute>
```

VEDERE ANCHE:

Informazioni sui provider di identità e i fornitori di servizi

## Utilizzo del registro eventi del provider di identità

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Developer Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Definire e modificare i provider di identità e i fornitori di servizi:

- "Personalizza applicazione"

Il registro eventi del provider di identità registra sia le operazioni eseguite che i problemi riscontrati nelle richieste di autenticazione SAML in entrata provenienti da un altro fornitore di applicazioni e nelle risposte SAML in uscita quando Salesforce funge da provider di identità. Per visualizzare il registro eventi del provider di identità, da Imposta, immettere `Registro evento provider di identità` nella casella `Ricerca veloce`, quindi selezionare **Registro evento provider di identità**. Nel registro è possibile visualizzare le operazioni riuscite, le operazioni non riuscite o entrambe. Si possono visualizzare i 50 eventi più recenti nell'interfaccia utente; per visualizzarne di più, creare un rapporto.

## Esempi di utilizzo dei provider di identità e dei fornitori di servizi

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Developer Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Database.com Edition**

Le schede non sono disponibili nella versione **Database.com Edition**

AUTORIZZAZIONI UTENTE

Definire e modificare i provider di identità e i fornitori di servizi:

- "Personalizza applicazione"

Questa sezione contiene due esempi di impostazione di Salesforce come provider di identità, quindi l'impostazione di due fornitori di servizi:

- Google Apps —mostra l'accesso avviato dal fornitore di servizi.
- Salesforce—mostra l'accesso avviato dal provider di identità.

### Impostazione del Single Sign-On a un esempio di Google Apps

Questo esempio mostra come impostare il Single Sign-On da Salesforce a Google Apps. In questo esempio, Google è il fornitore di servizi e Google Apps è l'applicazione fornita.

Affinché questo esempio funzioni, devono essere soddisfatte le seguenti condizioni:

- È necessario disporre di un account Google Apps Premier Edition
- L'organizzazione Salesforce deve essere configurata per Single Sign-On mediante SAML 2.0

Di seguito sono descritte le fasi generali, con maggiori dettagli a seguire dopo ogni fase.

1. Generare un nome di dominio e abilitare un provider di identità nell'organizzazione Salesforce.
2. Definire il fornitore di servizi in Salesforce.
3. Abilitare l'utente e il profilo di Salesforce.
4. Impostare Google Apps.
5. Verificare l'implementazione.

### Generazione di un nome di dominio e abilitazione di un provider di identità

Per preparare l'organizzazione Salesforce a questo esempio, generare un nome di dominio e abilitare Salesforce come provider di identità:

1. Accedere a Salesforce.
2. Generare un nome di dominio per la propria organizzazione:
   a. Da Imposta, digitare *`Dominio personale`* nella casella `Ricerca veloce`, quindi selezionare **Dominio personale**, immettere un nuovo nome di sottodominio e fare clic su **Verifica disponibilità**.
   b. Se il dominio è disponibile, fare clic sulla casella di controllo **Termini e condizioni** e quindi su **Registra dominio**.

   Importante: Prima di abilitare Salesforce come provider di identità, è necessario distribuire il nome di dominio.

3. Abilitare Salesforce come provider di identità:
   a. Da Imposta, immettere *`Provider di identità`* nella casella `Ricerca veloce`, quindi selezionare **Provider di identità**.
   b. Fare clic su **Abilita**.
   c. Fare clic su **Scarica certificati**. Ricordare la posizione nella quale si salva il certificato, in quanto verrà caricato in seguito.

### Definizione di un fornitore di servizi

Per definire il fornitore di servizi:

1. Accedere a Salesforce.
2. Da Imposta, immettere *`Applicazioni`* nella casella `Ricerca veloce`, quindi selezionare **Applicazioni**.
3. Fare clic su **Nuova** nella sezione Applicazioni connesse e in `Nome applicazione connessa` immettere `Google Apps`.
4. Nell'area Impostazioni app Web, selezionare **Abilita SAML** e quindi immettere le seguenti informazioni:

| Campo | Valore |
|---|---|
| `URL ACS` | L'URL dell'account Google App, ad esempio `https://www.google.com/a/respond.info` |
| `ID entità` | google.com |
| `Tipo di oggetto` | ID federazione |

5. Fare clic su **Salva**.
6. Per autorizzare l'accesso a questa applicazione, immettere *`Applicazioni connesse`* nella casella `Ricerca veloce`, selezionare l'opzione per la gestione delle applicazioni connesse e fare clic sul nome dell'applicazione. Selezionare il profilo utente corrente.
7. Copiare il valore nel campo `SP-Initiated Redirect Endpoint`. Questo valore verrà utilizzato in seguito.

### Mappatura dell'utente Salesforce all'utente Google Apps

1. Dalle impostazioni personali, immettere *`Dettagli utente avanzati`* nella casella `Ricerca veloce`, quindi selezionare **Dettagli utente avanzati**. Se non si ottiene alcun risultato, immettere *`Informazioni personali`* nella casella `Ricerca veloce`, quindi selezionare **Informazioni personali**.

2. Fare clic su **Modifica**.
3. Per `ID federazione`, immettere il nome utente utilizzato per l'accesso a Google Apps, ad esempio, GBianchi@TGroup.com.
4. Fare clic su **Salva**.

### Impostazione di Google Apps

1. Accedere all'account Google Apps.
2. Fare clic sulla scheda **Strumenti avanzati** e quindi sul link **Imposta Single Sign-On (SSO)**.
3. Selezionare la casella di controllo `Abilita Single Sign-On`.
4. Per `URL pagina di accesso`, immettere l'URL copiato dal campo `SP-Initiated Redirect Endpoint`, come descritto in definizione di un fornitore di servizi.
5. Per `URL pagina di disconnessione`, specificare l'URL al quale si desidera indirizzare gli utenti dopo la disconnessione da Google Apps, ad esempio `http://www.miodominio.salesforce.com`.
6. Per `Modifica URL password`, utilizzare il seguente URL: `https://miodominio.salesforce.com/_ui/system/security/ChangePassword`, dove *`miodominio`* è il nome specificato per il proprio dominio personalizzato al momento della generazione del dominio.
7. Per `Certificato di verifica`, caricare il certificato scaricato alla fase abilitazione di un provider di identità.
8. Fare clic su **Salva modifiche**.

### Verifica dell'implementazione

Per verificare che la propria organizzazione Salesforce possa utilizzare il Single Sign-On a Google Apps:

1. Disconnettersi da Google Apps e da Salesforce.
2. Provare ad accedere a una pagina Google App, ad esempio `http://docs.google.com/a/respond.info/` o `http://mail.google.com/a/respond.info/`.
3. Si verrà reindirizzati alla pagina di Single Sign-On di Salesforce. Dopo aver effettuato l'accesso, ci si trova alla pagina specificata di Google App.

Un'altra verifica può essere effettuata aggiungendo Google App a una scheda Web nell'organizzazione Salesforce.

1. Accedere a Salesforce.
2. Da Imposta, immettere *`Schede`* nella casella `Ricerca veloce`, quindi selezionare **Schede** e fare clic su **Nuova** nella sezione `Schede Web`.
3. Scegliere un layout per la scheda e fare clic su **Avanti**.
4. Immettere l'etichetta da visualizzare sulla scheda.
5. Utilizzare il nome predefinito, che equivale all'etichetta.
6. Fare clic sull'icona di ricerca `Stile scheda` per visualizzare il Selettore stile scheda. Selezionare un'icona. Lasciare invariate tutte le altre impostazioni predefinite.
7. Fare clic su **Avanti**.
8. Nella casella di testo URL pulsante o link, immettere una pagina Google App, ad esempio `docs.google.com/a/respond.info/` o `mail.google.com/a/respond.info/` e fare clic su **Avanti**.

   Nota: deve essere un URL assoluto, cioè deve contenere `http://` o `https://`.

9. Fare clic su **Avanti** e **Salva**.

10. Fare clic sulla nuova scheda nella parte superiore della pagina. Viene effettuato automaticamente l'accesso alla pagina Google App specificata.

## Impostazione di Single Sign-On da Salesforce a Salesforce

Questo esempio mostra come impostare un'applicazione Salesforce per avviare il Single Sign-On da un'organizzazione Salesforce a un'altra.

L'organizzazione Salesforce di avvio, cioè l'organizzazione che si desidera effettui l'accesso iniziale, funziona da *provider di identità*. L'organizzazione Salesforce che si desidera effettui l'accesso utilizzando un'applicazione funziona da *fornitore di servizi*. Ad esempio, si supponga di avere due organizzazioni Salesforce: un'organizzazione per le vendite e un'organizzazione per le idee. È possibile impostare il Single Sign-On tra le due organizzazioni in modo che gli utenti debbano soltanto accedere e ricordare la password di una di essa.

Per il corretto funzionamento di questo esempio, è necessario che l'organizzazione Salesforce di avvio sia configurata per il Single Sign-On utilizzando SAML 2.0 Di seguito sono descritte le fasi generali, con maggiori dettagli a seguire dopo ogni fase.

1. Generare un nome di dominio e abilitare un provider di identità nell'organizzazione Salesforce che funziona da provider di identità.
2. Impostare la propria organizzazione Salesforce che funziona da fornitore di servizi.
3. Definire l'applicazione del fornitore di servizi nell'organizzazione Salesforce che funziona da provider di identità.
4. Verificare l'implementazione.

## Generazione di un nome di dominio e abilitazione di un provider di identità

Tutte le operazioni descritte di seguito vengono effettuate nell'organizzazione Salesforce che funziona da provider di identità.

Per preparare l'organizzazione Salesforce a questo esempio, generare un nome di dominio e abilitare Salesforce come provider di identità:

1. Accedere a Salesforce.
2. Generare un nome di dominio per la propria organizzazione:
   a. Da Imposta, digitare `Dominio personale` nella casella `Ricerca veloce`, quindi selezionare **Dominio personale**, immettere un nuovo nome di sottodominio e fare clic su **Verifica disponibilità**.
   b. Se il dominio è disponibile, fare clic sulla casella di controllo **Termini e condizioni** e quindi su **Registra dominio**.

      Importante: Prima di abilitare Salesforce come provider di identità, è necessario distribuire il nome di dominio.

3. Abilitare Salesforce come provider di identità:
   a. Da Imposta, immettere `Provider di identità` nella casella `Ricerca veloce`, quindi selezionare **Provider di identità**.
   b. Fare clic su **Abilita**.
   c. Fare clic su **Scarica certificati**. Ricordare la posizione nella quale si salva il certificato, in quanto verrà caricato in seguito.

## Impostazione di un'organizzazione Salesforce come fornitore di servizi

Per configurare una seconda organizzazione Salesforce come fornitore di servizi:

1. Accedere all'organizzazione Salesforce che funziona da fornitore di servizi.
2. Abilitare e configurare SAML:
   a. Da Imposta, immettere `Impostazioni Single Sign-On` nella casella `Ricerca veloce`, quindi selezionare **Impostazioni Single Sign-On** e fare clic su **Modifica**.

b. Selezionare la casella di controllo `SAML abilitato`.

c. Utilizzare le seguenti impostazioni:

| Campo | Valore |
| --- | --- |
| `Versione SAML` | 2.0 |
| `Emittente` | URL emittente del provider di identità, creato quando viene impostato il provider di identità. Ad esempio, `https://dominiopersonalizzato.salesforce.com` |
| `Certificato provider identità` | Andare al certificato scaricato alla fase abilitazione di un provider di identità. |
| `Tipo ID utente SAML` | Selezionare `L'asserzione contiene l'ID federazione dell'oggetto utente` |
| `Posizione ID utente SAML` | Selezionare `L'ID utente è nell'elemento NameIdentifier dell'istruzione dell'oggetto` |

d. Fare clic su **Salva**.

e. Copiare e salvare i valori dai campi `URL di accesso Salesforce` e `ID entità`. Questi valori saranno richiesti in seguito, durante la definizione del fornitore di servizi Salesforce.

3. Collegare l'utente nell'organizzazione del fornitore di servizi all'utente nell'organizzazione del provider di identità:

a. Dalle impostazioni personali, immettere *Dettagli utente avanzati* nella casella `Ricerca veloce`, quindi selezionare **Dettagli utente avanzati**. Se non si ottiene alcun risultato, immettere *Informazioni personali* nella casella `Ricerca veloce`, quindi selezionare **Informazioni personali**.

b. Fare clic su **Modifica**.

c. Per `ID federazione`, immettere il nome utente utilizzato per l'accesso all'organizzazione del provider di identità Salesforce, ad esempio IDP_org@TGroup.com.

d. Fare clic su **Salva**.

## Definizione del provider di servizi nell'organizzazione del provider di identità

Per definire il provider di servizi, creare un'applicazione Web abilitata per SAML come applicazione connessa:

1. Accedere all'organizzazione Salesforce che funziona da provider di identità.
2. Da Imposta, immettere *Applicazioni* nella casella `Ricerca veloce`, selezionare **Applicazioni**, quindi, nella sezione Applicazioni connesse, fare clic su **Nuova**.
3. Specificare le seguenti informazioni:

| Campo | Valore |
| --- | --- |
| `Nome applicazione connessa` | Provider di servizi Salesforce |
| `Email referente` | Il referente che deve essere utilizzato da Salesforce per contattare l'utente o il suo team di assistenza. |

| Campo | Valore |
|---|---|
| `Abilita SAML` | Selezionare questa opzione per immettere i dettagli del provider di servizi. |
| `ID entità` | Utilizzare l'ID entità indicato in impostazione del fornitore di servizi |
| `URL ACS` | Utilizzare l'URL di accesso a Salesforce indicato in impostazione del fornitore di servizi |
| `Tipo di oggetto` | Selezionare `Nome utente`. |

4. Fare clic su **Salva**.
5. Selezionare i profili autorizzati ad accedere a questo fornitore di servizi. Per il corretto funzionamento di questo esempio, è necessario selezionare il profilo dell'utente corrente.
6. Fare clic su **Salva**.
7. Copiare il valore nel campo `IdP-Initiated Login URL`. Questo valore verrà utilizzato in seguito, durante la verifica.

## Verifica dell'implementazione

Per verificare che la propria organizzazione Salesforce possa utilizzare il Single Sign-On per la connessione, creare una scheda Web:

1. Accedere all'organizzazione Salesforce che funziona da fornitore di servizi.
2. Da Imposta, immettere *`Schede`* nella casella `Ricerca veloce`, quindi selezionare **Schede** e fare clic su **Nuova** nella sezione `Schede Web`.
3. Scegliere un layout per la scheda e fare clic su **Avanti**.
4. Immettere l'etichetta da visualizzare sulla scheda.
5. Utilizzare il nome predefinito, che equivale all'etichetta.
6. Fare clic sull'icona di ricerca `Stile scheda` per visualizzare il Selettore stile scheda. Selezionare un'icona.
7. Fare clic su **Avanti**.
8. Nella casella di testo URL pulsante o link, immettere il valore del campo `IdP-Initiated Login URL` indicato indefinizione del fornitore di servizi e fare clic su **Avanti**.

   Nota: deve essere un URL assoluto, cioè deve contenere `http://` o `https://`.

9. Fare clic su **Avanti** e **Salva**.
10. Fare clic sulla nuova scheda nella parte superiore della pagina. Se ci si è disconnessi dall'organizzazione Salesforce che funziona da provider di identità, viene richiesto di accedere. Una volta effettuato l'accesso, l'organizzazione Salesforce che funziona da provider di identità dovrebbe essere visibile nella scheda.

VEDERE ANCHE:

Informazioni sui provider di identità e i fornitori di servizi

## Configurazione delle impostazioni remote

Affinché una pagina Visualforce, una chiamata Apex o il codice JavaScript che utilizza XmlHttpRequest di un S-Control o di un pulsante personalizzato possano effettuare correttamente una chiamata a un sito esterno, tale sito deve essere registrato nella pagina Impostazioni sito remoto.

Per accedere alla pagina, da Imposta immettere *Impostazioni sito remoto* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni sito remoto**. La pagina visualizza un elenco di tutti i siti remoti già registrati e fornisce informazioni aggiuntive su ciascun sito, tra cui il nome e l'URL del sito remoto.

Per motivi di sicurezza, Salesforce limita le porte in uscita che si possono specificare a uno dei seguenti valori:

- 80: questa porta accetta solo connessioni HTTP.
- 443: questa porta accetta solo connessioni HTTPS.
- 1024-66535 (comprese): queste porte accettano connessioni HTTP o HTTPS.

Per registrare un nuovo sito:

1. Fare clic su **Nuovo sito remoto**.
2. Immettere un termine descrittivo per `Nome sito remoto`.
3. Immettere l'URL del sito remoto.
4. Per consentire l'accesso al sito remoto indipendentemente dal fatto che l'utente utilizzi una connessione HTTP o HTTPS, selezionare la casella di controllo `Disabilita sicurezza di protocollo`. Quando questa casella è selezionata, Salesforce può trasferire dati da una sessione HTTPS a una sessione HTTP e viceversa. Selezionare questa casella di controllo solo se si è coscienti delle sue implicazioni a livello di sicurezza.
5. Se lo si desidera, immettere una descrizione del sito.
6. Fare clic su **Salva** per terminare l'operazione, oppure su **Salva e Nuovo** per salvare il lavoro e iniziare la registrazione di un altro sito.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Visualforce e gli S-Control non sono disponibili nella versione **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per configurare le impostazioni remote:

- "Modifica tutti i dati"

## Credenziali denominate

### Credenziali denominate

Una credenziale denominata specifica l'URL di un callout endpoint e i relativi parametri obbligatori in una sola definizione. È possibile semplificare l'impostazione dei callout Apex autenticati specificando una credenziale denominata come callout endpoint. È anche possibile specificare un URL come callout endpoint e registrarlo nelle impostazioni del sito remoto dell'organizzazione. In questo caso, tuttavia, l'autenticazione viene gestita nel codice e ciò può garantire meno protezione e risultare particolarmente complicato per l'autenticazione OAuth.

Salesforce gestisce tutta l'autenticazione per i callout Apex che specificano una credenziale denominata come callout endpoint in modo tale che non lo faccia il codice. È inoltre possibile ignorare le impostazioni del sito remoto, che altrimenti sarebbero richieste per i callout Apex ai siti esterni.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **tutte** le versioni

Separando l'URL endpoint e l'autenticazione dal codice Apex, le credenziali denominate semplificano la gestione dei callout. Ad esempio, se un URL endpoint cambia, è sufficiente aggiornare la credenziale denominata. Tutti i callout che fanno riferimento alla credenziale denominata continuano a funzionare senza che vengano apportate modifiche al codice.

In caso vi siano più organizzazioni, è possibile creare una credenziale denominata con lo stesso nome in ogni organizzazione. Ognuna di queste credenziali denominate può avere un URL dell'endpoint diverso, ad esempio per tenere conto delle differenze tra gli ambienti di sviluppo e di produzione. Poiché il codice fa riferimento solo al nome delle credenziali denominate, è possibile creare e distribuire in un pacchetto la stessa classe Apex in tutte le organizzazioni senza verificare in modo programmatico l'ambiente.

Le credenziali denominate supportano l'autenticazione di base con password e OAuth 2.0. È possibile impostare ogni credenziale denominata in modo che utilizzi un direttore denominato a livello di organizzazione o l'autenticazione per utente per consentire agli utenti di gestire le proprie credenziali.

Esempio: Nell'esempio di codice che segue, una credenziale denominata e un percorso aggiunto specificano l'endpoint del callout.

```
HttpRequest req = new HttpRequest();
req.setEndpoint('callout:My_Named_Credential/some_path');
req.setMethod('GET');
Http http = new Http();
HTTPResponse res = http.send(req);
System.debug(res.getBody());
```

La credenziale denominata di riferimento specifica l'URL endpoint e le impostazioni di autenticazione.

Named Credential: My Named Credential

Help for this Page

Specify the callout endpoint's URL and the authentication settings that are required for Salesforce to make callouts to the remote system.

« Back to Named Credentials

Edit Delete

| | |
|---|---|
| Label | My Named Credential |
| Name | My_Named_Credential |
| URL | https://my_endpoint.example.com |

▼ Authentication

| | |
|---|---|
| Certificate | |
| Identity Type | Named Principal |
| Authentication Protocol | Password Authentication |
| Username | myname |

È possibile codificare il callout endpoint come URL anziché la credenziale denominata, ma in questo modo sarà il codice a gestire l'autenticazione. Questo esempio utilizza l'autenticazione di base con password, ma occorre tener presente che l'autenticazione OAuth è molto più complessa e viene gestita meglio con le credenziali denominate.

```
HttpRequest req = new HttpRequest();
req.setEndpoint('https://my_endpoint.example.com/some_path');
req.setMethod('GET');

// Because we didn't set the endpoint as a named credential,
// our code has to specify:
// - The required username and password to access the endpoint
// - The header and header information

String username = 'myname';
String password = 'mypwd';
```

```
Blob headerValue = Blob.valueOf(username + ':' + password);
String authorizationHeader = 'BASIC ' +
EncodingUtil.base64Encode(headerValue);
req.setHeader('Authorization', authorizationHeader);

// Create a new http object to send the request object
// A response object is generated as a result of the request

Http http = new Http();
HTTPResponse res = http.send(req);
System.debug(res.getBody());
```

VEDERE ANCHE:

Definizione di una credenziale denominata

Concessione dell'accesso alle impostazioni di autenticazione per le credenziali denominate

*Force.com Apex Code Developer's Guide*: Classe HttpRequest

## Definizione di una credenziale denominata

Creare una credenziale denominata per specificare l'URL di un callout endpoint e i relativi parametri obbligatori in una sola definizione. È possibile quindi specificare la credenziale denominata come callout endpoint Apex per consentire a Salesforce di gestire tutta l'autenticazione. È inoltre possibile ignorare le impostazioni del sito remoto, che altrimenti sarebbero richieste per i callout Apex ai siti esterni.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **tutte** le versioni

AUTORIZZAZIONI UTENTE

Per visualizzare, creare, modificare o eliminare credenziali denominate:

- "Modifica tutti i dati"

1. Da Imposta, immettere `Credenziali denominate` nella casella `Ricerca veloce`, quindi selezionare **Credenziali denominate**.
2. Fare clic su **Nuovo - Credenziale denominata** o su **Modifica** per modificare una credenziale denominata già esistente.
3. Compilare i campi.

| Campo | Descrizione |
|---|---|
| `Etichetta` | Nome intuitivo per la credenziale denominata visualizzata nell'interfaccia utente di Salesforce, ad esempio nelle visualizzazioni elenco.<br><br>Se si imposta `Tipo di identità` su Per utente, questa etichetta appare quando gli utenti visualizzano o modificano le impostazioni di autenticazione per i sistemi esterni. |
| `Nome` | Identificatore univoco utilizzato per fare riferimento a questa credenziale denominata dai callout Apex e tramite l'API.<br><br>Il nome può contenere solo caratteri di sottolineatura e alfanumerici. Deve essere univoco, iniziare con una lettera, non deve includere spazi, né terminare con un carattere di sottolineatura, né contenere due caratteri di sottolineatura consecutivi. |

<table>
<tr><th>Campo</th><th>Descrizione</th></tr>
<tr><td><code>URL</code></td><td>URL o URL principale del callout endpoint. Deve iniziare con <code>http://</code> o <code>https://</code>.<br><br>È possibile aggiungere un percorso specifico in ogni callout Apex. Ad esempio, se si crea la credenziale denominata "Mio_Esempio" e si imposta l'<code>URL</code> su <code>https://mio.esempio.com</code>, è possibile impostare come segue il callout Apex in modo che utilizzi un percorso specifico:<br><br><code>HttpRequest req = new HttpRequest();</code><br><code>req.setEndpoint('callout:My_Example/my/appended/path');</code></td></tr>
<tr><td><code>Certificato</code></td><td>Se si specifica un certificato, l'organizzazione Salesforce lo fornisce ad ogni connessione SSL bidirezionale con il sistema esterno. Il certificato viene utilizzato per le firme digitali, che verificano che le richieste provengano dall'organizzazione dell'utente.</td></tr>
<tr><td><code>Tipo di identità</code></td><td>Determina se si sta utilizzando un solo insieme o più insiemi di credenziali per accedere al sistema esterno.<ul><li>Anonimo: nessuna identità e quindi nessuna autenticazione.</li><li>Per utente: utilizzare credenziali separate per ogni utente che accede al sistema esterno tramite callout. Selezionare questa opzione se i limiti per l'accesso al sistema esterno sono suddivisi per utente.<br><br>Una volta concesso l'accesso tramite insiemi di autorizzazioni o profili in Salesforce, gli utenti possono gestire le proprie impostazioni di autenticazione per i sistemi esterni nelle impostazioni personali.</li><li>Direttore denominato: utilizzare lo stesso insieme di credenziali per tutti gli utenti che accedono al sistema esterno dalla propria organizzazione. Selezionare questa opzione se si dispone di un unico account utente designato sul sistema esterno che può essere utilizzato da tutti gli utenti dell'organizzazione per connettersi al sistema esterno.</li></ul></td></tr>
</table>

4. Selezionare il protocollo di autenticazione.
   - Se si seleziona **OAuth 2.0**, compilare i seguenti campi.

| Campo | Descrizione |
| --- | --- |
| `Provider di autenticazione` | Consente di scegliere il provider creato per questa credenziale denominata. |
| `Ambito` | Specifica l'ambito delle autorizzazioni da richiedere per il token di accesso. |
| `Avvia flusso di autenticazione al salvataggio` | Selezionare questa opzione per testare le credenziali quando si fa clic su **Salva**. |

   - Se si seleziona **Autenticazione password**, immettere il nome utente e la password per l'accesso al sistema esterno.

     Se è stato selezionato Per utente come `Tipo di identità`, le credenziali di amministrazione sono comunque richieste per consentire all'organizzazione di accedere al sistema esterno.

Per creare callout Apex a una credenziale denominata, utilizzare questo formato per il parametro *endpoint* nel metodo setEndpoint.

```
HttpRequest req = new HttpRequest();
req.setEndpoint('callout:My_Named_Credential/some_path');
```

VEDERE ANCHE:

Credenziali denominate

Concessione dell'accesso alle impostazioni di autenticazione per le credenziali denominate

*Force.com Apex Code Developer's Guide*: Classe HttpRequest

## Concessione dell'accesso alle impostazioni di autenticazione per le credenziali denominate

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **tutte** le versioni

AUTORIZZAZIONI UTENTE

Per modificare gli insiemi di autorizzazioni e i profili utente:

- "Gestisci profili e insiemi di autorizzazioni"

Per le credenziali denominate che utilizzano l'autenticazione basata sull'utente, è possibile concedere l'accesso agli utenti tramite gli insiemi di autorizzazioni e i profili. In questo modo gli utenti potranno impostare e gestire le proprie impostazioni di autenticazione per l'accesso al sistema esterno.

1. Da Imposta, immettere *Insiemi di autorizzazioni* nella casella Ricerca veloce, quindi selezionare **Insiemi di autorizzazioni** o **Profili**.
2. Fare clic sul nome dell'insieme di autorizzazioni o del profilo che si desidera modificare.
3. Eseguire una delle seguenti operazioni.
   - Per un insieme di autorizzazioni o per un profilo nell'interfaccia utente profilo ottimizzata, fare clic su **Accesso credenziale denominata** nella sezione delle applicazioni. Quindi, fare clic su **Modifica**.
   - Per un profilo nell'interfaccia utente profilo originale, fare clic su **Modifica** nella sezione relativa all'accesso alle credenziali denominate abilitate.
4. Aggiungere le credenziali denominate che si desidera abillitare.
5. Fare clic su **Salva**.

VEDERE ANCHE:

Definizione di una credenziale denominata

Credenziali denominate

# Identity Connect

## Informazioni su Identity Connect

Identity Connect fornisce l'integrazione con Active Directory.

Identity Connect consente l'integrazione di Active Directory con Salesforce tramite un servizio eseguibile indifferentemente su piattaforme Windows o Linux. Questa integrazione comprende la sincronizzazione degli utenti di Active Directory utilizzando Salesforce o Identity Connect come IDP (Identity Service Provider) per l'integrazione con Active Directory Single Sign-On (SSO) quando si accede a Salesforce.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile con un supplemento di prezzo nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition** La versione **Developer Edition** include 10 licenze per insiemi di autorizzazioni Identity Connect.

VEDERE ANCHE:

- https://na1.salesforce.com/help/pdfs/en/identity_connect_impl_guide.pdf
- Installazione di Identity Connect
- Abilitazione di Identity Connect

## Installazione di Identity Connect

L'organizzazione deve possedere almeno una licenza Identity Connect. Per ottenere Identity Connect, contattare Salesforce.

Il software Identity Connect viene normalmente installato su un server dal'ufficio IT. Gli utenti non devono installare singolarmente Identity Connect.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile con un supplemento di prezzo nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition** La versione **Developer Edition** include 10 licenze per insiemi di autorizzazioni Identity Connect.

AUTORIZZAZIONI UTENTE

Per installare Identity Connect:

- "Gestisci utenti"

1. Da Imposta, immettere `Identity Connect` nella casella `Ricerca veloce`, quindi selezionare **Identity Connect**.

   Nota: **Identity Connect** non appare in Imposta finché la funzione non viene aggiunta all'organizzazione in Salesforce.

2. Fare clic sul link per il download corrispondente al sistema operativo in uso.
3. Installare il software secondo le istruzioni della Salesforce Identity Connect Implementation Guide.

VEDERE ANCHE:

- Informazioni su Identity Connect
- Abilitazione di Identity Connect

## Abilitazione di Identity Connect

Per ottenere Identity Connect, contattare Salesforce.

Per abilitare Identity Connect per un utente:

1. Assegnare la licenza Identity Connect all'utente.
2. Creare un insieme di autorizzazioni e aggiungervi l'autorizzazione "Utilizza Identity Connect".
3. Assegnare l'insieme di autorizzazioni all'utente.

Guarda una dimostrazione: Creazione, modifica e assegnazione di un insieme di autorizzazioni

VEDERE ANCHE:

https://na1.salesforce.com/help/pdfs/en/identity_connect_impl_guide.pdf

Informazioni su Identity Connect

Installazione di Identity Connect

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile con un supplemento di prezzo nelle versioni: **Enterprise Edition**, **Performance Edition** e **Unlimited Edition** La versione **Developer Edition** include 10 licenze per insiemi di autorizzazioni Identity Connect.

AUTORIZZAZIONI UTENTE

Per assegnare una licenza insieme di autorizzazioni:

- "Gestisci utenti interni"

Per creare e assegnare gli insiemi di autorizzazioni:

- "Gestisci profili e insiemi di autorizzazioni"

Per visualizzare gli utenti assegnati a un insieme di autorizzazioni:

- "Visualizza impostazione e configurazione"

# Monitoraggio dell'organizzazione

## Informazioni sulla pagina di Panoramica del sistema

Nota: La pagina di panoramica del sistema mostra solo gli elementi abilitati per l'organizzazione. Ad esempio, la pagina di panoramica del sistema mostrerà le regole di flusso di lavoro solo se il flusso di lavoro è stato abilitato per l'organizzazione.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: tutte le versioni tranne **Personal Edition**

AUTORIZZAZIONI UTENTE

Per accedere alla pagina di panoramica del sistema:

- "Personalizza applicazione"

La pagina di panoramica del sistema mostra i dati e i limiti di utilizzo per l'organizzazione e visualizza i relativi messaggi quando si raggiunge il 95% del limite (75% dei ruoli dei portali). Per informazioni più dettagliate in merito all'utilizzo, fare clic sui numeri visualizzati sotto ogni metrica. Se disponibile, utilizzare Checkout per incrementare i limiti di utilizzo dell'organizzazione. Ad esempio, se l'organizzazione raggiunge il limite previsto per gli oggetti personalizzati, la pagina di panoramica del sistema notifica l'utente con un link di messaggio. Fare clic sul link per ripulire gli eventuali oggetti inutilizzati oppure visitare Checkout per incrementare il limite per gli oggetti.

Per accedere alla pagina della panoramica del sistema, da Imposta, digitare *`Panoramica del sistema`* nella casella `Ricerca veloce` e quindi selezionare **Panoramica del sistema**.

La pagina di panoramica del sistema visualizza i dati di utilizzo relativi a:

- Schema
- Utilizzo API
- Logica aziendale
- Interfaccia utente
- Licenze più utilizzate
- Ruoli portale

Nota: Le percentuali dei limiti degli oggetti vengono troncate, non arrotondate. Ad esempio, se l'organizzazione utilizza il 95,55% del limite per una determinata personalizzazione, il limite visualizzato per l'oggetto è 95%.

## Panoramica del sistema: Schema

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: tutte le versioni tranne **Personal Edition**

Il riquadro Schema nella pagina di panoramica del sistema mostra le informazioni di utilizzo relative a:

- Oggetti personalizzati

  Nota: Gli oggetti personalizzati e i relativi dati eliminati in modo non definitivo rientrano nel conteggio ai fini del raggiungimento dei limiti. Si consiglia di eliminare o cancellare definitivamente gli oggetti personalizzati non più necessari.

- Memoria dati

## Panoramica del sistema: Utilizzo API

Il riquadro Utilizzo API nella pagina della panoramica del sistema mostra le informazioni di utilizzo relative alle richieste API delle ultime 24 ore.

I limiti vengono imposti su tutte le chiamate API effettuate dall'organizzazione su un periodo di 24 ore; i limiti non sono suddivisi per utente. Quando un'organizzazione supera un limite, tutti gli utenti dell'organizzazione possono essere temporaneamente impossibilitati a effettuare altre chiamate. Le chiamate verranno bloccate finché l'utilizzo relativo alle 24 ore precedenti non scende al di sotto del limite.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

## Panoramica del sistema: Logica aziendale

Il riquadro Logica aziendale nella pagina di panoramica del sistema mostra le informazioni di utilizzo relative a:

- Regole
- Trigger Apex
- Classi Apex
- Codice utilizzato: il numero totale di caratteri utilizzati nei trigger e nelle classi Apex (ad esclusione dei commenti, dei metodi di test e delle classi annotate @isTest).

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

## Panoramica del sistema: Interfaccia utente

Il riquadro Interfaccia utente nella pagina di panoramica del sistema mostra le informazioni di utilizzo relative a:

- Applicazioni personalizzate
- Siti Site.com: vengono conteggiati solo i siti Site.com pubblicati.
- Siti Force.com attivi
- Flussi: Vengono conteggiati solo i flussi attivi.
- Schede personalizzate
- Pagine Visualforce

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: tutte le versioni tranne **Personal Edition** e Database.com Edition

## Panoramica del sistema: Licenze più utilizzate

Nel riquadro Licenze più utilizzate della pagina di panoramica del sistema vengono conteggiate solo le licenze attive e, per impostazione predefinita, vengono visualizzate le tre licenze più utilizzate dell'organizzazione. Inoltre, vengono visualizzate tutte le licenze che raggiungono un utilizzo del 95%. Fare clic su **Mostra tutto** per visualizzare tutte le licenze della propria organizzazione.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: tutte le versioni tranne **Personal Edition**

## Panoramica del sistema: Ruoli portale

Il riquadro Ruoli portale nella pagina di panoramica del sistema mostra i dati e il limite di utilizzo per la totalità dei ruoli del Portale partner, del Portale Clienti e delle comunità. La pagina di panoramica del sistema visualizza un messaggio quando l'organizzazione raggiunge il 75% dei ruoli del portale ad essa assegnati.

Nota: Il numero massimo di ruoli del portale per un'organizzazione è 5.000. Questo limite include i ruoli del portale associati a tutti i portali cliente, portali partner e comunità dell'organizzazione. Per evitare un incremento indesiderato di questo numero, consigliamo di rivedere e ridurre il numero dei ruoli per ogni portale e ogni comunità. Inoltre, si consiglia di eliminare gli eventuali ruoli del portale inutilizzati. Se si necessita comunque di ruoli del portale aggiuntivi, contattare l'Assistenza clienti di Salesforce.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

# Monitoraggio delle risorse

## Elementi che richiedono memoria

La memoria è divisa in due categorie: memoria file e memoria dati. La memoria file include i file contenuti negli allegati, nella scheda Documenti, nella scheda File, nel campo File, in Salesforce CRM Content, i file Chatter (comprese le foto degli utenti) e gli asset Site.com. La memoria dati contiene quanto segue:

- Account
- Tipi di articolo (formato: “[`Nome tipo di articolo`]”)
- Traduzioni tipi di articolo (formato: “[`Nome tipo di articolo`] Versione”)
- Campagne
- Membri campagna
- Casi
- Team caso
- Referenti
- Contratti
- Oggetti personalizzati
- Messaggi email
- Eventi

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile in: **tutte** le versioni

AUTORIZZAZIONI UTENTE

Per visualizzare l'utilizzo della memoria:

- "Gestisci utenti interni"

- Voci previsione
- Google Documenti
- Idee
- Lead
- Note
- Opportunità
- Ripartizioni opportunità
- Ordini
- Preventivi
- Dati RTF di modelli di preventivo
- Soluzioni
- Tag: Tag univoci
- Operazioni

## Capacità di memoria

Per la memoria file, alle versioni Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition e Unlimited Edition viene assegnato un limite per utente moltiplicato per il numero di utenti dell'organizzazione più un'ulteriore allocazione per organizzazione. Ad esempio, un'organizzazione Enterprise Edition con 600 utenti riceve 1211 GB di memoria file, o 2 GB per utente moltiplicato per 600 utenti, più altri 11 GB. Un'organizzazione Professional Edition con 600 utenti riceve circa 370 GB di memoria file, o 612 MB per utente moltiplicato per 600 utenti, più altri 11 GB.

Per la memoria dati, le versioni Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition e Unlimited Edition ricevono un limite di 1 GB o un limite per ogni utente, qualsiasi sia il valore più grande. Ad esempio, un'organizzazione Professional Edition con 10 utenti riceve 1 GB in quanto 10 utenti moltiplicati per 20 MB per ogni utente sarebbe pari a 200 MB, ossia meno del minimo di 1 GB. Un'organizzazione Professional Edition con 100 utenti riceve più del minimo di 1 GB in quanto 100 utenti moltiplicati per 20 MB per ogni utente è pari a 2.000 MB.

I valori indicati nella colonna Allocazione di memoria per licenza utente si riferiscono alle licenze utente Salesforce e Salesforce Platform.

| Versione di Salesforce | Memoria dati minima per organizzazione | Allocazione di memoria dati per licenza utente | Allocazione di memoria file per organizzazione | Allocazione di memoria file per licenza utente |
|---|---|---|---|---|
| Contact Manager | 1 GB | 20 MB | 11 GB | 612 MB |
| Group Edition | 1 GB | 20 MB | 11 GB | 612 MB |
| Professional Edition | 1 GB | 20 MB | 11 GB | 612 MB |
| Enterprise Edition | 1 GB | 20 MB | 11 GB | 2 GB |
| Prestazioni | 1 GB | 120 MB | 11 GB | 2 GB |
| Illimitato | 1 GB | 120 MB | 11 GB | 2 GB |
| Sviluppatore | 5 MB | N/D | 20 MB | N/D |
| Personal Edition | 20 MB (circa 10.000 record) | N/D | 20 MB | N/D |

Se l'organizzazione utilizza le licenze utente personalizzate, contattare Salesforce per capire se queste licenze offrono memoria aggiuntiva. Per una descrizione delle licenze utente, vedere Panoramica sulle licenze utente.

## Visualizzazione dell'utilizzo di memoria

Per visualizzare l'utilizzo di memoria corrente della propria organizzazione, da Imposta, immettere *Utilizzo della memoria* nella casella Ricerca veloce, quindi selezionare **Utilizzo della memoria**. È possibile visualizzare lo spazio di memoria dati e memoria file disponibile, la quantità di memoria in uso per tipo di record, gli utenti principali in termini di utilizzo della memoria e i file più grandi in ordine di dimensione. Per visualizzare quale tipo di dati viene memorizzato da un determinato utente, fare clic sul nome dell'utente.

In tutte le versioni, ad eccezione della versione Personal Edition, gli amministratori possono visualizzare l'utilizzo della memoria utente per utente:

1. Da Imposta, immettere *Utenti* nella casella Ricerca veloce, quindi selezionare **Utenti**.
2. Fare clic sul nome di un utente.
3. Fare clic su **Visualizza** accanto al campo Spazio dati utilizzato o accanto al campo Spazio file utilizzato per visualizzare l'utilizzo della memoria relativo a tale utente secondo il tipo di record.

La memoria dati e la memoria file vengono calcolate in modo asincrono e, se si importa o si aggiunge un numero elevato di record o di file, l'utilizzo della memoria dell'organizzazione non viene aggiornato immediatamente.

I singoli utenti possono visualizzare il proprio utilizzo della memoria nelle informazioni personali.

## Aumento della memoria

Se è necessario un maggior spazio di memoria, aumentare il limite di memoria o ridurre l'utilizzo della memoria.

- Acquistare spazio di memoria aggiuntivo, oppure aggiungere licenze utente nelle versioni Professional Edition, Enterprise Edition, Unlimited Edition e Performance Edition.
- Eliminare i lead o referenti superati.
- Eliminare gli allegati non necessari.
- Eliminare i file in Salesforce CRM Content.

## Considerazioni sullo spazio di memoria

Durante la pianificazione delle proprie esigenze di spazio, tenere presente quanto segue:

- Gli account personali vengono conteggiati sia nella memoria degli account che nella memoria dei referenti, poiché l'API presume che ogni account personale sia costituito da un account e da un referente.
- le attività archiviate vengono conteggiate nel calcolo dello spazio di memoria,
- I prodotti, i listini prezzi, le voci dei listini prezzi e gli asset attivi o archiviati non vengono conteggiati nel calcolo dello spazio di memoria.

# Monitoraggio della cronologia accessi

Gli amministratori possono monitorare tutti i tentativi di accesso per l'organizzazione e i portali o le comunità abilitate. La pagina della cronologia accessi visualizza gli ultimi 20.000 tentativi di accesso. Per visualizzare un maggior numero di record, scaricare i dati in un file in formato CSV o GZIP.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Contact Manager Edition**, **Developer Edition**, **Enterprise Edition**, **Group Edition**, **Performance Edition**, **Professional Edition** e **Unlimited Edition**

AUTORIZZAZIONI UTENTE

Per monitorare gli accessi:
- "Gestisci utenti"

## Download della cronologia accessi

È possibile scaricare gli ultimi sei mesi di accessi all'organizzazione Salesforce in un file CSV o GZIP.

1. Da Imposta, immettere *Cronologia accessi* nella casella `Ricerca veloce`, quindi selezionare **Cronologia accessi**.
2. Selezionare il formato di file da scaricare.
   - **File .csv Excel**: scarica un file CSV di tutti gli accessi degli utenti all'organizzazione Salesforce degli ultimi sei mesi. Questo rapporto è comprensivo degli accessi effettuati tramite API.
   - **File .csv Excel compresso con gzip**: scarica un file CSV di tutti gli accessi degli utenti all'organizzazione Salesforce degli ultimi sei mesi. Questo rapporto è comprensivo degli accessi effettuati tramite API. Il file è compresso e questa è l'opzione da preferirsi per ridurre i tempi di download.
3. Selezionare i contenuti del file. L'opzione Tutti gli accessi include gli accessi API.
4. Fare clic su **Scarica ora**,

Nota: le versioni meno recenti di Microsoft Excel non possono aprire file contenenti più di 65.536 righe. Se non è possibile aprire un file di grandi dimensioni in Excel, vedere l'articolo della Guida in linea e supporto tecnico di Microsoft sulla gestione dei file di grandi dimensioni.

## Creazione di visualizzazioni elenco

È possibile creare nuove visualizzazioni elenco ordinate per ora di accesso e URL di accesso. Ad esempio, è possibile creare una visualizzazione di tutti gli accessi in un particolare intervallo di tempo. Analogamente alla visualizzazione predefinita, una visualizzazione personalizzata visualizza gli ultimi 20.000 accessi.

1. Nella pagina Cronologia accessi, fare clic su **Crea nuova visualizzazione**.
2. Immettere il nome da visualizzare nell'elenco a discesa Visualizza.
3. Specificare i criteri di filtro.
4. Selezionare i campi da visualizzare.

   È possibile selezionare fino a 15 campi. È possibile visualizzare solo i campi disponibili nel proprio layout di pagina. I campi area di testo visualizzano fino a 255 caratteri.

   Nota: per via della natura della tecnologia di localizzazione geografica, la precisione dei campi di posizione geografica (ad esempio paese, città, codice postale) può variare.

## Visualizzazione della cronologia accessi personale

È possibile visualizzare la cronologia accessi personale.

1. Dalle impostazioni personali, immettere *Cronologia accessi* nella casella Ricerca veloce, quindi selezionare **Cronologia accessi**. Se non si ottiene alcun risultato, immettere *Informazioni personali* nella casella Ricerca veloce, quindi selezionare **Informazioni personali**.
2. Per scaricare un file CSV della cronologia degli accessi personali degli ultimi sei mesi, fare clic su **Download...**

Nota: Per motivi di sicurezza, Salesforce potrebbe richiedere agli utenti di superare un test di verifica CAPTCHA per poter esportare i dati dalla propria organizzazione. Questo semplice test impedisce ai programmi dannosi di accedere ai dati della propria organizzazione. Per superare il test, gli utenti devono digitare correttamente le due parole visualizzate nella sovrapposizione all'interno della casella di testo. Tenere presente che le parole immesse nella casella di testo devono essere separate da uno spazio.

## Single Sign-On con SAML

Se l'organizzazione utilizza i certificati del provider di identità Single Sign-On SAML, gli accessi Single Sign-On saranno inclusi nella cronologia.

## Dominio personale

Se si utilizza Dominio personale, è possibile identificare gli utenti che accedono con il nuovo URL di accesso, nonché il momento dell'accesso. Da Imposta, immettere *Cronologia accessi* nella casella Ricerca veloce, quindi selezionare **Cronologia accessi** e visualizzare le colonne Nome utente e URL di accesso.

# Monitoraggio della cronologia formazione

Per un amministratore è importante sapere se il proprio team sta imparando a utilizzare Salesforce in modo efficace. Nella Cronologia corso di formazione sono visualizzati tutti i corsi di formazione di Salesforce frequentati dagli utenti.

Gli amministratori possono visualizzare la Cronologia corso di formazione da Imposta immettendo *Cronologia formazione* nella casella Ricerca veloce, quindi selezionando **Cronologia formazione**. Dopo aver frequentato un corso di formazione live, gli utenti devono compilare l'apposito modulo di commento sulla formazione online per ottenere la registrazione della presenza nella cronologia formazione.

Nota: Se questo link non appare in **Gestisci utenti**, l'organizzazione è stata migrata a un nuovo sistema. Per accedere ai rapporti sulla formazione tramite Casi personali in Assistenza e Formazione è necessario essere un amministratore di Assistenza e Formazione. Contattare Salesforce se non dispone dell'accesso.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare la cronologia della formazione:
- "Gestisci utenti"

# Monitoraggio delle modifiche di impostazione

La cronologia dell'itinerario di controllo delle impostazioni consente di tenere traccia delle modifiche recenti apportate alle impostazioni dell'organizzazione da parte dell'utente o di altri amministratori. La cronologia di controllo può rivelarsi particolarmente utile nelle organizzazioni con più amministratori.

Per visualizzare la cronologia dell'itinerario di controllo, da Imposta, immettere `Visualizza itinerario di controllo impostazioni` nella casella `Ricerca veloce`, quindi selezionare **Visualizza itinerario di controllo impostazioni**. Per eseguire il download della cronologia completa delle impostazioni dell'organizzazione relativa agli ultimi 180 giorni, fare clic sul link **Scarica**.

La cronologia dell'itinerario di controllo delle impostazioni consente di visualizzare le 20 più recenti modifiche di impostazione apportate all'organizzazione. Vengono visualizzati data, autore e natura della modifica. Inoltre, se un delegato (ad esempio un amministratore o un rappresentante dell'assistenza clienti) effettua una modifica di impostazione per conto di un utente finale, la colonna Utente delegato visualizza il nome utente del delegato. Ad esempio, se un utente concede l'accesso a un amministratore e questi effettua una modifica di impostazione, viene elencato il nome utente dell'amministratore.

La cronologia dell'itinerario di controllo delle impostazioni tiene traccia dei seguenti tipi di modifiche:

| Impostazione | Modifiche di cui viene tenuta traccia |
| --- | --- |
| Amministrazione | • Informazioni sulla società, impostazioni predefinite quali la lingua o le impostazioni internazionali e modifiche al messaggio aziendale<br>• Modifiche alle impostazioni di più valute<br>• Modifiche agli utenti, agli utenti portale, ai ruoli, agli insiemi di autorizzazioni e ai profili<br>• Modifiche agli indirizzi email di ciascun utente<br>• Eliminazione degli allegati email inviati come link<br>• Creazione, modifica ed eliminazione piè di pagina email<br>• Modifiche al tipo di record, incluse creazione, ridenominazione o assegnazione dei tipi di record ai profili<br>• Modifiche alle divisioni, inclusi creazione, modifica, trasferimento di divisioni e modifica della divisione predefinita degli utenti<br>• Aggiunta o eliminazione di certificati<br>• Modifica dei nomi di dominio<br>• Abilitazione o disabilitazione di Salesforce come provider di identità |
| Personalizzazione | • Modifiche alle impostazioni dell'interfaccia utente, come ad esempio sezioni comprimibili, creazione rapida, dettagli effetto di attivazione o link effetto di attivazione elenco correlato<br>• Modifiche ai layout di pagina, di azione e di ricerca<br>• Modifiche ai layout compatti<br>• Modifiche al menu di navigazione di Salesforce1<br>• Cambiamenti apportati mediante modifica in linea |

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare la cronologia dell'itinerario di controllo:

- "Visualizza impostazione e configurazione"

| Impostazione | Modifiche di cui viene tenuta traccia |
| --- | --- |
| | • Modifiche relative ai campi personalizzati e alla protezione a livello di campo, comprese le modifiche a formule, valori di elenchi di selezione e attributi di campi personalizzati quali il formato dei campi a numerazione automatica, la gestibilità o la maschera dei campi crittografati<br>• Modifiche alle impostazioni dei lead, regole di assegnazione dei lead e aree di attesa lead<br>• Modifiche alle impostazioni delle attività<br>• Modifiche alle impostazioni di assistenza, orario di ufficio, regole di assegnazione dei casi e di inoltro al livello superiore e aree di attesa casi<br>• Qualsiasi modifica apportata dall'Assistenza clienti di Salesforce su richiesta dell'utente<br>• Modifiche ai nomi delle schede, incluse le schede reimpostate sul nome originale<br>• Modifiche alle applicazioni personalizzate (comprese le applicazioni di Salesforce Console), agli oggetti personalizzati e alle schede personalizzate<br>• Modifiche alle impostazioni dei contratti<br>• Modifiche alle impostazioni delle previsioni<br>• Abilitazione o disabilitazione di Email a caso o Email a caso on-demand<br>• Modifiche ai pulsanti, link e S-Control personalizzati, compreso il fatto di ignorare i pulsanti standard<br>• Abilitazione o disabilitazione di pianificazione trascinamento della selezione<br>• Abilitazione, disabilitazione o personalizzazione di opportunità simili<br>• Abilitazione o disabilitazione di preventivi<br>• Modifiche ai gruppi di categorie di dati, categorie di dati e assegnazioni di gruppi di categorie agli oggetti<br>• Modifiche di tipi di articoli<br>• Modifiche di gruppi di categorie e categorie<br>• Modifiche alle impostazioni di Salesforce Knowledge<br>• Modifiche alle impostazioni delle idee<br>• Modifiche alle impostazioni delle risposte<br>• Modifiche al tracciamento dei campi nei feed<br>• Modifiche alle impostazioni dell'influenza campagna<br>• Attivazione o disattivazione di aggiornamenti critici<br>• Abilitazione o disabilitazione delle notifiche tramite email di Chatter<br>• Abilitazione o disabilitazione delle impostazioni di creazione nuovo utente di Chatter per gli inviti e i domini di email<br>• Modifiche alle regole di convalida |
| Sicurezza e condivisione | • Modifiche ai gruppi pubblici, alle regole di condivisione e condivisione a livello di tutta l'organizzazione, inclusa l'opzione **Concedi accesso tramite le gerarchie**<br>• Modifiche ai criteri delle password<br>• Reimpostazioni delle password<br>• Modifiche alle impostazioni di sessione, ad esempio al timeout di sessione<br>• Modifiche ai gruppi di amministratori delegati e agli elementi che possono essere gestiti dagli amministratori delegati (viene tenuta traccia anche delle modifiche apportate dagli amministratori delegati alle impostazioni)<br>• Numero di record che un utente ha rimosso dal relativo Cestino e dal Cestino dell'organizzazione |

| Impostazione | Modifiche di cui viene tenuta traccia |
| --- | --- |
| | • Modifiche alle impostazioni di configurazione SAML (Security Assertion Markup Language)<br>• Modifiche dei certificati Salesforce<br>• Abilitazione o disabilitazione dei provider di identità<br>• Modifiche alle credenziali denominate<br>• Modifiche ai fornitori di servizi<br>• Modifiche all'impostazione di Crittografia piattaforma. |
| Gestione dati | • Utilizzo dell'eliminazione globale, compreso il caso in cui un'eliminazione globale supera il limite del Cestino dell'utente di 5000 record eliminati. I record meno recenti vengono rimossi definitivamente dal Cestino entro due ore dall'ora della transazione di eliminazione globale.<br>• Richieste di esportazione dati<br>• Utilizzo dell'importazione guidata dei membri campagna<br>• Utilizzo del trasferimento globale<br>• Modifiche alle istantanee dei rapporti, incluse la definizione, la rimozione o la modifica del rapporto origine o dell'oggetto di destinazione su un'istantanea del rapporto<br>• Utilizzo dell'Importazione guidata |
| Sviluppo | • Modifiche alle classi e ai trigger Apex<br>• Modifiche alle pagine, componenti personalizzati o risorse statiche di Visualforce<br>• Modifiche alle pagine Lightning<br>• Modifiche ai modelli di link azioni<br>• Modifiche alle impostazioni personalizzate<br>• Modifiche ai tipi di metadati e ai record personalizzati<br>• Modifiche alle definizioni di accesso remoto<br>• Modifiche alle impostazioni di Force.com Sites |
| Impostazioni varie | • Creazione di una notifica di misurazione dell'utilizzo API<br>• Modifiche ai territori<br>• Modifiche alle impostazioni di automazione dei processi<br>• Modifiche ai processi di approvazione<br>• Creazione ed eliminazione di azioni del flusso di lavoro<br>• Modifiche dei file Visual Workflow<br>• Pacchetti di Force.com AppExchange installati o disinstallati dall'utente |
| Utilizzo dell'applicazione | • Modifiche alle impostazioni del team account e della vendita in team opportunità<br>• Attivazione dei Servizi Google Apps<br>• Modifiche alle impostazioni di configurazione mobile, inclusi le serie di dati, le visualizzazioni mobili e i campi esclusi<br>• Utente dotato dell'autorizzazione "Gestisci utenti esterni" che accede al portale partner come utente partner |

| Impostazione | Modifiche di cui viene tenuta traccia |
| --- | --- |
| | • Utente dotato dell'autorizzazione "Modifica utenti Self-Service" che accede al Portale Clienti Salesforce come utente del Portale Clienti<br>• Abilitazione e disabilitazione di un account portale partner<br>• Disabilitazione di un account Portale Clienti Salesforce<br>• Abilitazione o disabilitazione di un Portale Clienti Salesforce e creazione di più Portali Clienti<br>• Creazione e modifica dei processi di diritti e dei modelli di diritti<br>• Abilitazione o disabilitazione dell'auto registrazione per un Portale Clienti Salesforce<br>• Abilitazione e disabilitazione di utenti del Portale Clienti o portale partner |

# Tieni traccia cronologia campo

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Gli oggetti standard non sono disponibili nella versione **Database.com Edition**

È possibile selezionare campi specifici di cui tenere traccia e visualizzare la cronologia dei campi nell'elenco correlato Cronologia di un oggetto. I dati della cronologia dei campi vengono conservati per un massimo di 18 mesi. È possibile tenere traccia della cronologia dei campi degli oggetti personalizzati e della cronologia dei seguenti oggetti standard.

- Account
- Asset
- Casi
- Referenti
- Diritti
- Contratti di servizio
- Voci di contratto
- Contratti
- Lead
- Opportunità
- Articoli
- Soluzioni
- Prodotti

Modificando uno di questi campi si aggiunge una voce all'elenco correlato Cronologia. Tutte le voci includono data, ora, tipo e autore della modifica. Non tutti i tipi di campo sono disponibili per i rapporti con trend storico. Alcune modifiche, come gli inoltri al livello superiore dei casi, vengono sempre tracciate.

Nota: Per gli incrementi della cronologia dei campi oltre i limiti correnti è necessario acquistare il componente aggiuntivo Itinerario di controllo campi, successivo al rilascio Spring '15. Dopo aver abilitato l'abbonamento del componente aggiuntivo, l'archivio della cronologia dei campi viene modificato per riflettere i criteri di conservazione associati all'offerta. Se l'organizzazione è stata creata prima del mese di giugno 2011 e i limiti della cronologia dei campi rimangono statici, Salesforce si impegna a conservare la cronologia dei campi illimitatamente. Se l'organizzazione è stata creata dopo il mese di giugno 2011 e si decide di non acquistare il componente aggiuntivo, la cronologia dei campi viene conservata per un massimo di 18 mesi.

## Considerazioni

- Le modifiche apportate ai campi con oltre 255 caratteri vengono rilevate nella cronologia come modifiche, ma i vecchi e i nuovi valori non vengono registrati.
- I valori dei campi di cui si tiene traccia non vengono tradotti automaticamente e vengono visualizzati nella lingua in cui sono stati creati. Ad esempio, se un campo viene modificato da *Green* a *Verde*, viene visualizzato *Verde* indipendentemente dalla lingua dell'utente, a meno che il campo sia stato tradotto in altre lingue tramite l'Area di lavoro traduzione. Questo vale anche per tipi di record e valori di elenchi di selezione.
- Le modifiche apportate a etichette di campi personalizzati che sono state tradotte tramite l'Area di lavoro traduzione vengono visualizzate in base alle impostazioni internazionali dell'utente che sta visualizzando l'elenco correlato Cronologia. Ad esempio, se l'etichetta di un campo personalizzato è `Rosso` ed è stata tradotta in spagnolo con `Rojo`, un utente che dispone di impostazioni internazionali Spagnolo visualizza l'etichetta del campo personalizzato come `Rojo`. In caso contrario, l'utente la visualizza come `Rosso`.
- Le modifiche apportate a campi data, campi numero e campi standard vengono visualizzate in base alle impostazioni internazionali dell'utente che sta visualizzando l'elenco correlato Cronologia. Ad esempio, una data modificata in *5 agosto 2012* verrà visualizzata come *8/5/2012* da un utente con le impostazioni internazionali Inglese (Stati Uniti) e come *5/8/2012* da un utente con le impostazioni internazionali Inglese (Regno Unito).
- Se un trigger causa una modifica in un oggetto che l'utente corrente non è autorizzato a modificare, la modifica non viene tracciata poiché la cronologia dei campi rispetta le autorizzazioni dell'utente corrente.

VEDERE ANCHE:

Tracciamento della cronologia dei campi per oggetti standard

Tracciamento della cronologia dei campi per oggetti personalizzati

Itinerario di controllo campi

Disabilitazione del tracciamento della cronologia dei campi

# Tracciamento della cronologia dei campi per oggetti standard

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Gli oggetti standard non sono disponibili nella versione **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per impostare i campi di cui viene tenuta traccia:

- "Personalizza applicazione"

Se si utilizzano sia gli account aziendali che gli account personali, riesaminare i seguenti punti prima di abilitare il tracciamento della cronologia dei campi di un account:

- Il tracciamento della cronologia dei campi degli account interessa sia gli account aziendali sia gli account personali.
- L'abilitazione del tracciamento della cronologia dei campi degli account personali non abilita il tracciamento della cronologia dei campi dei referenti personali.

Per impostare il tracciamento della cronologia dei campi:

1. Dalle impostazioni di gestione dell'oggetto di cui si desidera tracciare la cronologia dei campi, accedere all'area dei campi.
2. Fare clic su **Imposta tracciamento cronologia**.

   Suggerimento: quando si abilita il tracciamento per un oggetto, personalizzare i layout di pagina in modo da includere l'elenco correlato Cronologia dell'oggetto.

3. Per account, referenti, lead e opportunità, selezionare la casella di controllo `Abilita cronologia account`, `Abilita cronologia referenti`, `Abilita cronologia lead` o `Abilita cronologia campo opportunità`.
4. Scegliere i campi da tracciare.

   È possibile selezionare una combinazione di un massimo di 20 campi standard e personalizzati per oggetto. Tale limite include campi di account aziendali e account personali.

   Alcune modifiche, come gli inoltri al livello superiore dei casi, vengono sempre tracciate.

   Non è consentito tenere traccia dei seguenti campi:

   - Campi formula, riepilogo di roll-up o numerazione automatica
   - `Creato da` e `Ultima modifica di`
   - Campo `Reddito previsto` nelle opportunità
   - Campi `Titolo soluzione principale` o `Dettagli soluzione principale` nelle soluzioni; questi campi vengono visualizzati solo per le soluzioni tradotte nelle organizzazioni in cui sono abilitate le soluzioni multilingue.

5. Fare clic su **Salva**.

   Salesforce traccia la cronologia da questa data e ora. Le modifiche precedenti non vengono incluse.

VEDERE ANCHE:

Tieni traccia cronologia campo

# Tracciamento della cronologia dei campi per oggetti personalizzati

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Gli oggetti standard non sono disponibili nella versione **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per impostare i campi di cui viene tenuta traccia:

- "Personalizza applicazione"

1. Dalle impostazioni di gestione dell'oggetto personalizzato, fare clic su **Modifica**.
2. Selezionare la casella di controllo `Tieni traccia cronologia campo`.

   Suggerimento: quando si abilita il tracciamento per un oggetto, personalizzare i layout di pagina in modo da includere l'elenco correlato Cronologia dell'oggetto.

3. Salvare le modifiche.
4. Fare clic su `Imposta tracciamento cronologia` nella sezione Campi e relazioni personalizzati.

   Questa sezione consente di impostare la cronologia di un oggetto personalizzato per i campi standard e personalizzati.

5. Scegliere i campi da tracciare.

   È possibile selezionare un massimo di 20 campi standard e personalizzati per oggetto. Non è possibile tenere traccia dei seguenti campi:

   - Campi formula, riepilogo di roll-up o numerazione automatica
   - `Creato da` e `Ultima modifica di`

6. Fare clic su **Salva**.

   Salesforce traccia la cronologia da questa data e ora. Le modifiche precedenti non vengono incluse.

VEDERE ANCHE:

Tieni traccia cronologia campo

## Disabilitazione del tracciamento della cronologia dei campi

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Gli oggetti standard non sono disponibili nella versione **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per impostare i campi di cui viene tenuta traccia:

- "Personalizza applicazione"

Nota: non è possibile disabilitare il tracciamento della cronologia dei campi per un oggetto se Apex fa riferimento a uno dei campi dell'oggetto.

1. Dalle impostazioni di gestione dell'oggetto per cui si desidera interrompere il tracciamento della cronologia dei campi, accedere a Campi.
2. Fare clic su `Imposta tracciamento cronologia`.
3. Deselezionare **Abilita cronologia** per l'oggetto in uso, ad esempio **Abilita cronologia account**, **Abilita cronologia referenti**, **Abilita cronologia lead** o **Abilita cronologia opportunità**.

   L'elenco correlato Cronologia viene automaticamente rimosso dai layout di pagina dell'oggetto associato.

   Se in un oggetto standard si disabilita il tracciamento della cronologia dei campi, è comunque possibile eseguire un rapporto sui dati cronologici fino alla data e all'ora in cui il tracciamento è stato disabilitato. Se si disabilita il tracciamento della cronologia dei campi per un oggetto personalizzato, non è più possibile eseguire rapporti sulla sua cronologia dei campi.
4. Salvare le modifiche.

VEDERE ANCHE:

Tieni traccia cronologia campo

## Itinerario di controllo campi

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per specificare un criterio di conservazione della cronologia dei campi:

- "Conserva cronologia campi"

L'itinerario di controllo campi consente di definire un criterio per la conservazione dei dati della cronologia dei campi fino a 10 anni, indipendentemente dal tracciamento della cronologia. Questa funzionalità aiuta a mantenere la conformità con i regolamenti del settore relativi alle funzionalità di controllo e alla conservazione dei dati.

Utilizzare l'API metadati di Salesforce per definire un criterio di conservazione per la cronologia dei campi. Quindi utilizzare API REST, API SOAP e Tooling API per lavorare con i dati archiviati. Per informazioni sull'abilitazione di Itinerario controllo campi, contattare il rappresentante Salesforce.

La cronologia viene copiata dall'elenco correlato Cronologia nell'oggetto `FieldHistoryArchive` e quindi eliminata dall'elenco correlato Cronologia. Definire un solo oggetto `HistoryRetentionPolicy` per gli elenchi correlati delle cronologie, ad esempio Cronologia account, per specificare diversi criteri di conservazione dell'itinerario di controllo campi per gli oggetti che si desidera archiviare. Quindi, è possibile distribuire l'oggetto utilizzando l'API metadati (Workbench o Strumento di migrazione Force.com). Nelle organizzazioni di produzione con l'itinerario di controllo campi abilitato, i dati vengono archiviati per impostazione predefinita dopo 18 mesi. Nelle organizzazioni Sandbox l'impostazione predefinita è un mese. I criteri di conservazione possono essere aggiornati ogni volta che lo si desidera.

I criteri per l'itinerario di controllo campi possono essere impostati per i seguenti oggetti:

- Account
- Casi
- Referenti
- Lead
- Opportunità
- Oggetti personalizzati con tracciamento della cronologia dei campi abilitato

È possibile includere i criteri di conservazione della cronologia dei campi nei pacchetti gestiti e non gestiti.

Il tracciamento non è possibile per i seguenti campi.

- Campi formula, riepilogo di roll-up o numerazione automatica
- Creato da e Ultima modifica di
- Campo Reddito previsto nelle opportunità
- Campi Titolo soluzione principale o Dettagli soluzione principale nelle soluzioni
- Campi di testo lungo
- Campi a selezione multipla

Dopo aver definito e distribuito un criterio per l'itinerario di controllo campi, i dati di produzione vengono migrati dagli elenchi correlati della cronologia, come Cronologia account, all'oggetto `FieldHistoryArchive`. La prima copia scrive la cronologia dei campi definita dal criterio nella memoria in archivio e a volte richiede molto tempo. Le copie successive trasferiscono solo le modifiche apportate dopo l'ultima copia e vengono eseguite molto più rapidamente. È disponibile un insieme di istruzioni SOQL collegate per l'esecuzione di query sui dati archiviati.

Nota: per un certo periodo di tempo dopo il rilascio GA iniziale, è possibile che i dati non vengano eliminati automaticamente dall'elenco correlato Cronologia e restino sia nell'oggetto `FieldHistoryArchive` che nell'elenco correlato Cronologia. Salesforce si riserva il diritto di eliminare i dati archiviati dall'elenco correlato Cronologia in conformità ai criteri definiti dal cliente nei rilasci futuri.

**Nota:** Se l'organizzazione ha abilitato l'itinerario di controllo campi, i dati archiviati in precedenza non vengono crittografati se successivamente si attiva Crittografia piattaforma. Si immagini ad esempio che l'organizzazione usi l'itinerario di controllo campi per definire un criterio di conservazione della cronologia dei dati per un campo account come il campo del numero di telefono. Dopo avere abilitato Crittografia piattaforma si abilita la crittografia per quel campo e il numero di telefono dell'account viene crittografato. I record dei nuovi numeri di telefono vengono crittografati alla loro creazione, e i precedenti aggiornamenti del campo numero di telefono archiviati nell'elenco correlato Cronologia account vengono anch'essi crittografati. Invece, i dati cronologici relativi ai numeri di telefono già archiviati nell'oggetto `FieldHistoryArchive` continuano a restare senza crittografia. Se l'organizzazione ha l'esigenza di crittografare dei dati archiviati in precedenza, rivolgersi a Salesforce. I dati cronologici dei campi archiviati vengono crittografati e riarchiviati e l'archivio non crittografato viene eliminato.

VEDERE ANCHE:

*SOAP API Developer's Guide*: FieldHistoryArchive

*Metadata API Developer's Guide*: HistoryRetentionPolicy

*ISVforce Guide*: Panoramica sui pacchetti

*Force.com SOQL and SOSL Reference*: SOQL con i dati archiviati

## Esempi

### Impostazione di un criterio di conservazione dei dati per la cronologia dei campi

Questo esempio dimostra come impostare un criterio di conservazione dei dati per la cronologia dei campi utilizzando l'API dei metadati. La modifica dei metadati è necessaria solo se si desidera bypassare i valori dei criteri predefiniti (18 mesi di memoria di produzione e 0 anni di memoria di archivio). L'impostazione di un criterio di conservazione dei dati implica la creazione e la distribuzione di un pacchetto di metadati. Il pacchetto è costituito da un file `.zip` che contiene una cartella `objects` con l'XML che definisce il criterio di conservazione di ciascun oggetto e un file project manifest che elenca gli oggetti e la versione API da usare.

**Nota:** La prima copia scrive l'intera cronologia dei campi definita dal criterio nella memoria in archivio e potrebbe richiedere molto tempo. Le copie successive trasferiscono solo le modifiche apportate dopo l'ultima copia e vengono eseguite molto più rapidamente.

1. Definire un criterio di conservazione dei dati della cronologia dei campi per ciascun oggetto. Il criterio specifica il numero di mesi per i quali si desidera conservare la cronologia dei campi in Salesforce, oltre al numero di anni per i quali si desidera conservare la cronologia dei campi nell'archivio. Il file di esempio seguente definisce un criterio di conservazione dell'oggetto dopo sei mesi e per la conservazione degli archivi per cinque anni.

```
<?xml version="1.0" encoding="UTF-8"?>
<CustomObject xmlns="http://soap.sforce.com/2006/04/metadata">
   <historyRetentionPolicy>
       <archiveAfterMonths>6</archiveAfterMonths>
       <archiveRetentionYears>5</archiveRetentionYears>
       <description>My field history retention</description>
   </historyRetentionPolicy>
   <fields>
       <fullName>AccountSource</fullName>
...
</CustomObject>
```

   Il nome del file determina l'oggetto a cui viene applicato il criterio. Ad esempio, per applicare il criterio di cui sopra all'oggetto Account, salvare il file come `Account.object`. Per gli oggetti personalizzati esistenti il procedimento è identico, con il file denominato in base all'oggetto personalizzato. Ad esempio: `myObject__c.object`.

2. Creare il file project manifest, che è un file XML chiamato `package.xml`. Il seguente file di esempio elenca diversi oggetti ai quali applicare il criterio di conservazione dei dati. Con questo file manifest, ci si aspetta che la cartella degli oggetti contenga cinque file: `Account.object`, `Case.object` e così via.

```
<?xml version="1.0" encoding="UTF-8"?>
<Package xmlns="http://soap.sforce.com/2006/04/metadata">
    <types>
        <members>Account</members>
        <members>Case</members>
        <members>Contact</members>
        <members>Lead</members>
        <members>Opportunity</members>
    </types>
    <version>32.0</version>
</Package>
```

3. Creare il file `.zip` e utilizzare la funzione `deploy()` per distribuire le modifiche all'ambiente di produzione. Per ulteriori informazioni, vedere Metadata API Guide.

   Nota: questa funzione pilota non supporta la distribuzione dagli ambienti Sandbox a quelli di produzione.

Fatto! Il criterio di conservazione della cronologia dei campi entrerà in vigore in base ai periodi di tempo impostati.

## Creazione di un oggetto personalizzato e impostazione di un criterio di conservazione della cronologia dei campi nello stesso momento

È possibile utilizzare l'API dei metadati per creare un oggetto personalizzato e impostare contemporaneamente un criterio di conservazione. Quando si crea un nuovo oggetto personalizzato è necessario specificare i campi minimi richiesti. Ecco un XML di esempio che crea un oggetto e imposta il criterio di conservazione della cronologia dei campi:

```
<?xml version="1.0" encoding="UTF-8"?>
<CustomObject xmlns="http://soap.sforce.com/2006/04/metadata">
    <deploymentStatus>Deployed</deploymentStatus>
    <enableHistory>true</enableHistory>
    <description>just a test object with one field for eclipse ide testing</description>
    <historyRetentionPolicy>
        <archiveAfterMonths>3</archiveAfterMonths>
        <archiveRetentionYears>10</archiveRetentionYears>
        <gracePeriodDays>1</gracePeriodDays>
        <description>Transaction Line History</description>
    </historyRetentionPolicy>
    <fields>
        <fullName>Comments__c</fullName>
        <description>add your comments about this object here</description>
       <inlineHelpText>This field contains comments made about this object</inlineHelpText>

        <label>Comments</label>
        <length>32000</length>
        <trackHistory>true</trackHistory>
        <type>LongTextArea</type>
        <visibleLines>30</visibleLines>
    </fields>
    <label>MyFirstObject</label>
    <nameField>
```

```
        <label>MyFirstObject Name</label>
        <type>Text</type>
    </nameField>
    <pluralLabel>MyFirstObjects</pluralLabel>
    <sharingModel>ReadWrite</sharingModel>
</CustomObject>
```

Impostare `trackHistory` su `true` per i campi di cui si desidera tenere traccia e su `false` per gli altri campi.

### Esecuzione di query sui dati archiviati

È possibile recuperare i dati archiviati eseguendo delle query SOQL sull'oggetto `FieldHistoryArchive`. È possibile filtrare in base ai campi `FieldHistoryType`, `ParentId` e `CreatedDate`, purché li si specifichi in questo ordine. Ad esempio:

```
SELECT ParentId, FieldHistoryType, Field, Id, NewValue, OldValue FROM FieldHistoryArchive
 WHERE FieldHistoryType = 'Account' AND ParentId='906F000000
```

VEDERE ANCHE:

*Metadata API Developer's Guide*: deploy()

*Metadata API Developer's Guide*: CustomObject

*Force.com SOQL and SOSL Reference*: SOQL con i dati archiviati

## Monitoraggio dei registri debug

Dopo aver impostato i propri flag di traccia, monitorare la registrazione per utenti, classi Apex e trigger Apex nella Console sviluppatore o in Imposta.

È possibile conservare e gestire i registri debug per utenti specifici, inclusi se stessi, e per le classi e i trigger.

Per visualizzare i registri debug salvati, da Imposta, immettere *Registri debug* nella casella `Ricerca veloce`, quindi selezionare **Registri debug**. Dopo aver iniziato a conservare i registri debug, è possibile visualizzare, scaricare o eliminare i propri registri da questa pagina.

VEDERE ANCHE:

Impostazione della registrazione debug

Visualizzazione dei registri debug

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

L'interfaccia utente e i Servizi di email di Salesforce non sono disponibili nella versione **Database.com Edition**.

AUTORIZZAZIONI UTENTE

Per visualizzare, conservare ed eliminare i registri debug:

- "Gestisci utenti"

# Impostazione della registrazione debug

Per attivare i registri debug per utenti, classi Apex e trigger Apex, configurare i flag di traccia e i livelli debug nella Console sviluppatore o in Imposta.

È possibile conservare e gestire i registri debug per utenti specifici, inclusi se stessi, e per le classi e i trigger.

Per i registri debug esistono i seguenti limiti.

- Ogni registro debug deve avere dimensioni massime pari a 2 MB. Le dimensioni dei registri debug che superano 2 MB vengono ridotte rimuovendo le righe di registro più vecchie, quali le righe di registro delle dichiarazioni `System.debug` precedenti. Le righe di registro possono essere eliminate da qualsiasi posizione, non soltanto dal registro debug.
- Ogni organizzazione può conservare fino a 50 MB di registri debug. Quando l'organizzazione raggiunge il limite di 50 MB, i registri debug più vecchi vengono sovrascritti.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare, conservare ed eliminare i registri debug:
- "Gestisci utenti"

## Configurazione dei flag di traccia nella Console sviluppatore

Per configurare i flag di traccia e i livelli debug dalla Console sviluppatore, fare clic su **Debug** > **Change Log Levels (Cambia livelli di registrazione)**. Quindi eseguire la procedura descritta di seguito.

- Per creare un flag di traccia, fare clic su **Add (Aggiungi)**.
- Per modificare la durata di un flag di traccia esistente, fare doppio clic sulla sua ora di inizio o di fine.
- Per modificare il livello debug di un flag di traccia, fare clic su **Add/Change (Aggiungi/Modifica)** nella colonna Debug Level Action (Azione livello debug). È quindi possibile modificare i propri livelli debug esistenti, creare un livello debug e assegnare un livello debug al proprio flag di traccia.

## Configurazione dei flag di traccia in Imposta

Per configurare i flag di traccia e i livelli debug da Imposta, eseguire la seguente procedura.

1. Accedere alla pagina Imposta appropriata.
   - Per i flag di traccia e i livelli debug basati sugli utenti, immettere *`Registri debug`* nella casella `Ricerca veloce`, quindi selezionare **Registri debug**.
   - Per i flag di traccia e i livelli debug basati sulle classi, immettere *`Classi Apex`* nella casella `Ricerca veloce`, fare clic su **Classi Apex**, fare clic sul nome di una classe, quindi su **Flag di traccia**.
   - Per i flag di traccia e i livelli debug basati sui trigger, immettere *`Trigger Apex`* nella casella `Ricerca veloce`, fare clic su **Trigger Apex**, fare clic sul nome di una classe, quindi su **Flag di traccia**.
2. Dalla pagina Imposta, eseguire la seguente procedura.
   - Per aggiungere un flag di traccia, fare clic su **Nuovo**.
   - Per modificare un flag di traccia esistente, fare clic su un'opzione nella colonna Azione.
     - Per eliminare un flag di traccia, fare clic su **Rimuovi**.
     - Per modificare un flag di traccia, fare clic su **Modifica**.
     - Per modificare il livello debug di un flag di traccia, fare clic su **Filtri**.

- Per creare un livello debug, fare clic su **Modifica**, fare clic sull'icona a forma di lente di ingrandimento accanto al campo Livello debug e quindi fare clic su **Nuovo**.

VEDERE ANCHE:

Monitoraggio dei registri debug

## Visualizzazione dei registri debug

AUTORIZZAZIONI UTENTE

| | |
|---|---|
| Per utilizzare la Console sviluppatore: | "Visualizza tutti i dati" |
| Per eseguire Apex Code anonimo: | "Apex autore" |
| Per utilizzare la ricerca nel codice ed eseguire SOQL o SOSL nella scheda della query: | "API abilitata" |
| Per salvare le modifiche alle classi e ai trigger Apex: | "Apex autore" |
| Per salvare le modifiche alle pagine e ai componenti Visualforce: | "Personalizza applicazione" |
| Per salvare le modifiche delle risorse Lightning: | "Personalizza applicazione" |

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Per visualizzare i dettagli di un registro debug, da Imposta immettere *Registri debug* nella casella Ricerca veloce, selezionare **Registri debug** e quindi fare clic su **Visualizza** accanto al registro debug da esaminare. Fare clic su **Scarica** per scaricare il registro sotto forma di file XML.

Il registro debug contiene informazioni sulla transazione, ad esempio il suo esito, le dimensioni del registro (in byte), la durata della transazione in millisecondi e così via. Il registro in sé contiene informazioni aggiuntive sulla transazione, a seconda dei filtri impostati per l'utente.

VEDERE ANCHE:

Monitoraggio dei registri debug

# Monitoraggio di processi pianificati

La pagina Tutti i processi pianificati elenca tutte le istantanee del rapporto, tutti i processi Apex pianificati e tutti i cruscotti digitali con aggiornamento pianificato.

Per visualizzare questa pagina, da Imposta, immettere *`Processi pianificati`* nella casella `Ricerca veloce` e selezionare **Processi pianificati**. A seconda delle autorizzazioni di cui si dispone, è possibile eseguire alcune o tutte le azioni riportate di seguito.

- Fare clic su **Canc** per eliminare definitivamente tutte le istanze di un processo pianificato.
- Visualizzare i dettagli di un processo pianificato, ad esempio:
  - Nome del processo pianificato
  - Nome dell'utente che ha inviato il processo pianificato
  - Data e ora in cui il processo pianificato è stato inviato in origine
  - Data e ora in cui il processo pianificato è iniziato
  - Data e ora in cui il processo pianificato verrà eseguito la prossima volta
  - Tipo di processo pianificato

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

Istantanee del rapporto e cruscotti digitali non sono disponibili nella versione **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per monitorare i processi pianificati:

- "Visualizza impostazione e configurazione"

# Monitoraggio dei processi in background

È possibile monitorare i processi in background se per l'organizzazione è stato abilitato il ricalcolo parallelo della condivisione. Il ricalcolo parallelo della condivisione consente alle organizzazioni più grandi di velocizzare il ricalcolo della condivisione di ogni oggetto. Nel rilascio Winter '14, il ricalcolo parallelo è disponibile automaticamente in tutte le nuove organizzazioni. Le organizzazioni esistenti possono contattare Salesforce per determinare se questa funzionalità è appropriata per la propria azienda.

Per visualizzare i processi in background della propria organizzazione, da Imposta digitare *Processi in background* nella casella Ricerca veloce, quindi selezionare **Processi in background**.

La pagina Tutti i processi in background contiene i dettagli relativi ai processi eseguiti in background, compresa una stima in percentuale dell'avanzamento del ricalcolo. La colonna **Tipo di processo** mostra il processo in background in esecuzione, ad esempio Aggiornamento impostazioni predefinite organizzazione. La colonna **Sottotipo di processo** mostra l'oggetto interessato, ad esempio Account o Opportunità.

Nota: In questa pagina è possibile soltanto monitorare i processi in background. Per interrompere un processo in background, rivolgersi a Salesforce.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per monitorare i processi in background:
- "Visualizza impostazione e configurazione"

VEDERE ANCHE:

Ricalcolo delle regole di condivisione

Ricalcolo parallelo asincrono delle regole di condivisione

# Configurazione delle applicazioni Salesforce Mobile

## Salesforce1

### Considerazioni sull'impostazione dell'app mobile Salesforce1

Esistono numerose opzioni che consentono di personalizzare l'app mobile Salesforce1, in modo da trasformarla in un efficace strumento mobile su misura per gli utenti.

Tutte le opzioni di personalizzazione di Salesforce1 sono disponibili dal menu Imposta, cui si accede dall'angolo in alto a destra di qualsiasi pagina Salesforce. Per comodità, è possibile accedere più rapidamente a molte pagine delle impostazioni di Salesforce1 dalla pagina di impostazione Avvio rapido di Salesforce1. In Salesforce Classic, da Imposta, fare clic su **Avvio rapido di Salesforce1**. In Lightning Experience, da Imposta immettere *Avvio rapido di Salesforce1* nella casella Ricerca veloce, quindi selezionare **Avvio rapido di Salesforce1**.

Nota: si consiglia di utilizzare Google Chrome per la pagina di impostazione Avvio rapido di Salesforce1. Sono supportati anche Microsoft Internet Explorer 9 o versione successiva e Mozilla Firefox.

Di seguito sono illustrate le opzioni di personalizzazione di Salesforce1 che è possibile prendere in esame per la propria organizzazione.

EDIZIONI

Disponibile in Lightning Experience nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Disponibile in Salesforce Classic in: **tutte** le versioni tranne Database.com Edition

- Procedere ad alcune impostazioni di base utilizzando la Procedura guidata di Salesforce1. Nella pagina Avvio rapido di Salesforce1, fare clic su **Lancia la Procedura guidata di avvio rapido**.
- Definire gli utenti che possono accedere a Salesforce1.
  - Per le applicazioni scaricabili, dalla pagina Avvio rapido di Salesforce1, fare clic su **Controlli di protezione app**.
  - Per l'applicazione browser mobile, dalla pagina Avvio rapido di Salesforce1, fare clic su **Opzione browser mobile**.
- Personalizzare il modo in cui i dati sono visualizzati in Salesforce1. Se non diversamente specificato, è possibile accedere a queste personalizzazioni dalle impostazioni di gestione dell'oggetto di cui si vogliono personalizzare i dati.
  - Ottimizzare i layout di pagina in modo che vengano visualizzati bene sui dispositivi mobili. È possibile modificare i layout di pagina esistenti oppure creare layout di pagina nuovi e idonei per dispositivi mobili. Dalle impostazioni di gestione dell'oggetto appropriato, accedere a Layout di pagina.
  - Aggiungere ricerche estese, componenti (tra cui Twitter) o pagine Visualforce alla sezione Schede mobili di un layout di pagina per visualizzarli come schede mobili in Salesforce1. Dalle impostazioni di gestione dell'oggetto appropriato, accedere a Layout di pagina.
  - Assicurarsi che le pagine Visualforce siano abilitate per l'uso in Salesforce1, in modo tale che appaiano nell'app. Da Imposta, immettere *Pagine Visualforce* nella casella `Ricerca veloce`, quindi selezionare **Pagine Visualforce**. Fare clic su **Modifica** accanto al nome di una pagina, quindi selezionare `Disponibile per le applicazioni mobili Salesforce`.
  - Definire i campi da visualizzare nell'area di evidenziazione dei record di un oggetto e nelle schede di anteprima degli elenchi correlati, creando layout compatti personalizzati. Dalle impostazioni di gestione dell'oggetto appropriato, accedere a Layout compatti.
  - Verificare che i layout di ricerca esistenti compilino i risultati della ricerca di Salesforce1 utilizzando i campi desiderati. Dalle impostazioni di gestione dell'oggetto appropriato, accedere a Layout di ricerca.
- Per rendere più facile ed efficiente l'uso dei campi, è possibile creare azioni su misura per le attività aziendali e i casi di uso specifici.
  - Abilitare le azioni nel publisher per la propria organizzazione. Da Imposta, immettere *Impostazioni Chatter* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni Chatter**. Selezionare la casella di controllo `Abilita le azioni nel publisher`. (Ciò presume che nella propria organizzazione sia abilitato Chatter e che si desideri che le azioni create appaiano nel publisher Chatter. Se per la propria organizzazione non è stato abilitato Chatter, le azioni possono essere utilizzate ma verranno visualizzate solo in Salesforce1 e non sul sito Salesforce completo).

    Nota: se le azioni publisher non sono abilitate, nel publisher Chatter del sito Salesforce completo vengono visualizzate solo le azioni Chatter standard (Post, File, Link, Sondaggio e Ringraziamenti). Quando Chatter è abilitato ma le azioni nel publisher sono disabilitate, le azioni standard e non standard di Chatter vengono visualizzate nella barra delle azioni in Salesforce1 e nelle applicazioni di terzi che utilizzano gli elenchi di azioni. Le azioni non standard includono le azioni Crea, Aggiorna, Registra una chiamata, le azioni personalizzate e le azioni intelligenti dispositivo mobile.

  - Creare azioni globali che consentano agli utenti di aggiungere nuovi record di oggetti senza relazioni automatiche ad altri record. Da Imposta, immettere `Azioni globali` nella casella `Ricerca veloce`, quindi selezionare **Azioni globali**. Per personalizzare i campi utilizzati dalle azioni globali, fare clic su **Layout** nella pagina Azioni globali.

    Quindi, aggiungere le nuove azioni alla sezione Azioni di Salesforce1 e Lightning Experience del layout publisher globale, in modo che vengano visualizzate in Salesforce1. Da Imposta, immettere `Layout publisher` nella casella `Ricerca veloce`, quindi selezionare **Layout publisher**.

  - Creare azioni specifiche degli oggetti che consentono agli utenti di aggiungere nuovi record o aggiornare i dati nei record già esistenti. Dalle impostazioni di gestione dell'oggetto a cui si desidera aggiungere un'azione, accedere a Pulsanti, Link e Azioni. Per personalizzare i campi utilizzati da un'azione specifica di un oggetto, fare clic su **Layout** nella pagina Pulsanti, Link e Azioni.

Quindi, aggiungere le nuove azioni alla sezione Azioni di Salesforce1 e Lightning Experience del layout di pagina dell'oggetto in questione.

- Personalizzare le opzioni disponibili nel menu di navigazione di Salesforce1 nonché l'ordine in cui appaiono le voci. Dalla pagina Avvio rapido di Salesforce1, fare clic su **Menu di navigazione**.
- Fare in modo che gli utenti di Salesforce1 vengano a conoscenza di attività importanti di Salesforce abilitando le notifiche all'interno dell'applicazione (in-app) e le notifiche push. Dalla pagina Avvio rapido di Salesforce1, fare clic su **Opzioni di notifica**.
- Integrare le app di terze parti nel menu di navigazione di Salesforce1 aggiungendo schede Lightning Page per le Lightning Page distribuite all'organizzazione. Da Imposta, immettere `Schede` nella casella `Ricerca veloce`, quindi selezionare **Schede** e fare clic su **Nuova** nell'elenco correlato Schede della pagina Lightning.
- Personalizzare Salesforce1 in modo tale che rifletta l'immagine aziendale della propria società. Dalla pagina Avvio rapido di Salesforce1, fare clic su **Immagine aziendale Salesforce1**.
- Consentire alle app scaricabili di Salesforce1 di inserire automaticamente nella cache i dati di Salesforce ai quali si accede più spesso per una memorizzazione sicura e permanente, in modo che gli utenti possano visualizzare i dati quando i loro dispositivi sono offline. (Questa opzione è abilitata per impostazione predefinita.) Dalla pagina Avvio rapido di Salesforce1, fare clic su **Cache offline**.

Può inoltre essere utile consultare la *guida all'amministrazione delle app mobili di Salesforce1*, che fornisce istruzioni dettagliate sull'uso degli strumenti dichiarativi di Salesforce1 in Imposta per preparare l'organizzazione all'esperienza mobile con Salesforce1.

VEDERE ANCHE:

Impostazione dell'app mobile Salesforce1 con la procedura guidata Salesforce1

## Impostazione dell'app mobile Salesforce1 con la procedura guidata Salesforce1

La Procedura guidata Salesforce1 offre un modo semplice per completare le operazioni essenziali di impostazione di Salesforce1. Dopo aver impostato Salesforce1 utilizzando questa procedura guidata, gli agenti di vendita potranno utilizzare Salesforce1 per gestire le loro attività dai dispositivi mobili.

> **Nota:** Si consiglia di utilizzare Google Chrome per la procedura guidata di Salesforce1 e la pagina Impostazione di Salesforce1. Sono supportati anche Microsoft Internet Explorer 9 o versione successiva e Mozilla Firefox.

Se si utilizza Lightning Experience:

1. Da Imposta, fare clic su **Lancia l'importazione guidata** nel riquadro Imposta Salesforce1 nell'area di accesso rapido.

Se si utilizza Salesforce Classic:

1. Da Imposta, fare clic su **Avvio rapido di Salesforce1**.
2. Nella pagina Impostazione di Salesforce1, fare clic su **Lancia la Procedura guidata di avvio rapido**.

> **Nota:** benché la Procedura guidata di Salesforce1 consenta di avviare ed eseguire le operazioni di impostazione di base, non include tutte le operazioni di impostazione di Salesforce1. Ad esempio, benché sia possibile riorganizzare le azioni rapide globali tramite la procedura guidata, la barra delle azioni e il menu delle azioni di Salesforce1 possono includere altri tipi di azioni, ad esempio le azioni rapide specifiche degli oggetti e le azioni Chatter standard, a seconda del contesto.

EDIZIONI

Disponibile in Lightning Experience nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Disponibile in Salesforce Classic in: **tutte** le versioni tranne Database.com Edition

AUTORIZZAZIONI UTENTE

Per utilizzare la Procedura guidata di Salesforce1:
- "Personalizza applicazione"

Al termine della procedura guidata, si verrà indirizzati alla pagina di impostazione Avvio rapido di Salesforce1, che fornisce facile accesso alle pagine di impostazione e alla documentazione di Salesforce1. Per le impostazioni configurate su una pagina singola, la pagina Avvio rapido include link diretti a tali pagine. Per i casi in cui le impostazioni sono disponibili su più pagine in Imposta, abbiamo fornito i link alla documentazione pertinente sull'impostazione.

VEDERE ANCHE:

Considerazioni sull'impostazione dell'app mobile Salesforce1

## Controllo dell'accesso all'app mobile Salesforce1

È possibile controllare l'accesso dell'organizzazione alle app scaricabili di Salesforce1 e all'app browser mobile Salesforce1.

In base alla configurazione della propria organizzazione, è possibile:

- Abilitare o disabilitare l'accesso all'app browser mobile Salesforce1. Da Imposta, immettere *Impostazioni Salesforce1* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni Salesforce1**. Vedere Abilitazione dell'app browser mobile Salesforce1.
- Stabilire chi può accedere alle app scaricabili di Salesforce1 e configurare altre policy di sicurezza. Da Imposta, immettere *Applicazioni connesse* nella casella `Ricerca veloce`, quindi selezionare l'opzione di gestione delle applicazioni connesse. Vedere Policy di accesso utenti e sicurezza per le app scaricabili di Salesforce1.

EDIZIONI

Disponibile in Lightning Experience nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Disponibile in Salesforce Classic in: **tutte** le versioni tranne Database.com Edition

## Policy di accesso utenti e sicurezza per le app scaricabili di Salesforce1

EDIZIONI

Disponibile in Lightning Experience nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Disponibile in Salesforce Classic in: **tutte** le versioni tranne Database.com Edition

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni dell'app scaricabile di Salesforce1:

- "Personalizza applicazione"

Per visualizzare le impostazioni dell'app scaricabile di Salesforce1:

- "Visualizza impostazione e configurazione"

Le app scaricabili di Salesforce1 sono applicazioni connesse. Di conseguenza, è possibile controllare gli utenti che hanno accesso alle app, nonché altre policy sulla sicurezza. Per impostazione predefinita, tutti gli utenti dell'organizzazione possono accedere alle app scaricabili di Salesforce1.

È possibile controllare le policy di sicurezza e accesso per ciascuna app scaricabile di Salesforce1, utilizzando i componenti di impostazione installati dal pacchetto gestito di applicazioni connesse di Salesforce1. I seguenti componenti devono essere installati in Salesforce:

- Salesforce1 per Android
- Salesforce1 per iOS

Tali componenti vengono automaticamente installati quando uno degli utenti installa un'app scaricabile di Salesforce1 da App Store o Google Play su un dispositivo mobile ed esegue l'autenticazione con l'organizzazione mediante l'accesso all'app mobile.

In alternativa, è possibile installare manualmente il pacchetto di applicazioni connesse di Salesforce1 e Chatter in modo da rivedere e modificare le impostazioni predefinite relative alla sicurezza e all'accesso prima di distribuire le app scaricabili di Salesforce1 agli utenti.

All'installazione, i componenti delle applicazioni connesse di Salesforce1 vengono aggiunti alla pagina Applicazioni connesse (da Imposta, immettere *Applicazioni connesse* nella casella Ricerca veloce, quindi selezionare l'opzione di gestione delle applicazioni connesse). Qui è possibile visualizzare e modificare le impostazioni per ciascuna applicazione, incluso il controllo dell'accesso degli utenti con profili, autorizzazioni e restrizioni dell'intervallo IP. Viene visualizzato un messaggio di errore se un utente con accesso limitato tenta di accedere a un'app scaricabile di Salesforce1.

Le notifiche push per le app scaricabili di Salesforce1 non vengono gestite dalla pagina Applicazioni connesse. Per gestire queste impostazioni, da Imposta immettere *Notifiche* nella casella Ricerca veloce, quindi selezionare **Notifiche in Salesforce1**.

L'accesso offline viene abilitato per impostazione predefinita quando è installata una delle app scaricabili di Salesforce1. Per gestire queste impostazioni, da Imposta immettere *Offline* nella casella Ricerca veloce, quindi selezionare **Salesforce1 Offline**.

VEDERE ANCHE:

Abilitazione delle notifiche dell'app mobile Salesforce1

## Abilitazione dell'app browser mobile Salesforce1

È possibile stabilire se gli utenti possono accedere all'app browser mobile Salesforce1 quando accedono a Salesforce da un browser mobile. Per impostazione predefinita, l'app browser mobile è attivata per l'organizzazione.

Importante: l'uso del sito Salesforce Classic completo in un browser mobile non è supportato. L'app browser mobile Salesforce1 può essere disabilitata per l'organizzazione e i singoli utenti possono disattivarla per sé; tuttavia, non è consigliabile utilizzare regolarmente il sito completo in un browser mobile. Gli utenti potrebbero riscontrare dei problemi su cui l'Assistenza clienti di Salesforce non indagherà.

Non è possibile accedere al sito completo di Lightning Experience da nessun browser mobile.

1. Da Imposta, immettere *Impostazioni Salesforce1* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni Salesforce1**.
2. Selezionare `Abilita l'app browser mobile Salesforce1` per consentire agli utenti dell'organizzazione di accedere all'app. Deselezionare questa opzione per disattivare l'accesso all'app.
3. Fare clic su **Salva**.

Quando questa opzione è attiva, gli utenti che accedono a Salesforce da un browser mobile supportato vengono indirizzati automaticamente all'interfaccia di Salesforce1. Se si accede da un browser mobile non supportato, viene caricato il sito Salesforce Classic completo anche quando questa opzione è stata selezionata.

EDIZIONI

Disponibile in Lightning Experience nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Disponibile in Salesforce Classic in: **tutte** le versioni tranne Database.com Edition

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni dell'app browser mobile Salesforce1:
- "Visualizza impostazione e configurazione"

Per modificare le impostazioni dell'app browser mobile Salesforce1:
- “Personalizza applicazione”

  "Modifica tutti i dati"

## Menu di navigazione dell'app mobile Salesforce1

Di seguito sono descritte le voci visualizzate nel menu di navigazione di Salesforce1. È possibile personalizzare la maggior parte delle caratteristiche del menu di navigazione per la propria organizzazione.

L'icona nell'intestazione di Salesforce1 consente di aprire il menu di navigazione.

EDIZIONI

Disponibile in Lightning Experience nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Disponibile in Salesforce Classic in: **tutte** le versioni tranne Database.com Edition

Se il menu di navigazione predefinito non soddisfa le esigenze degli utenti, è possibile personalizzarlo. Da Imposta, immettere *Navigazione in Salesforce1* nella casella `Ricerca veloce`, quindi selezionare **Navigazione in Salesforce1**.

A seconda delle impostazioni dell'organizzazione, il menu può contenere le seguenti opzioni:

| Voce di menu | Descrizione |
|---|---|
| Richieste di approvazione | Visualizza un elenco delle approvazioni in sospeso dell'utente. Gli utenti possono toccare una voce approvazione e approvarla o rifiutarla da Salesforce1. Disponibile nell'app scaricabile Salesforce1 per iOS e nell'app browser mobile Salesforce1. |
| App dell'area di disegno | Visualizzata per le organizzazioni che hanno abilitato la visualizzazione di un'app area di disegno nel menu di navigazione di Salesforce1. |
| Cruscotti digitali | La disponibilità dipende dalla versione e dalle autorizzazioni utente. Se non si include questa voce nel menu, nel gruppo Elementi di ricerca intelligente viene aggiunta automaticamente una voce Cruscotti digitali. |
| Eventi | Elenca gli eventi di cui l'utente è titolare, che l'utente ha creato per sé e a cui l'utente o i suoi gruppi sono invitati. |
| Feed | Visualizzata per le organizzazioni con Chatter abilitato. |
| Scheda Componente Lightning (Beta) | Solo i componenti Lightning personalizzati a cui è associata una scheda Componente Lightning possono comparire nel menu di navigazione di Salesforce1. |
| Pagine Lightning | Pagine dell'app Salesforce1 personalizzate. |
| Gruppi | Visualizzata per le organizzazioni con Chatter abilitato. Se non si include questa voce nel menu, nel gruppo Elementi di ricerca intelligente viene aggiunta automaticamente una voce Gruppi. |

| Voce di menu | Descrizione |
|---|---|
| Interviste del flusso in pausa | Visualizza un elenco di interviste del flusso che l'utente ha messo in pausa. Un'intervista è un'istanza in esecuzione di un flusso. Gli utenti possono toccare un'intervista e riprenderla o eliminarla da Salesforce1. Disponibile solo nell'app browser mobile Salesforce1. |
| Persone | Visualizzata per le organizzazioni con Chatter abilitato. Se non si include questa voce nel menu, nel gruppo Elementi di ricerca intelligente viene aggiunta automaticamente una voce Persone. |
| Elementi di ricerca intelligente | Aggiunge oggetti Salesforce alla sezione Recenti del menu. Questa voce inserisce inoltre una serie di oggetti cercati di recente nella sezione Recenti e aggiunge la voce Altro per consentire agli utenti di accedere a tutti gli oggetti che sono autorizzati a utilizzare e che sono supportati in Salesforce1. Se non si inserisce questa voce nel menu di navigazione, gli utenti non potranno accedere ad alcun oggetto in Salesforce1.<br>Nota: inizialmente, se per un utente non esiste ancora una cronologia di oggetti recenti, nella sezione Recenti è visualizzata una serie di oggetti predefiniti. Possono essere necessari fino a 15 giorni prima che gli oggetti utilizzati regolarmente sia in Salesforce1, sia nel sito Salesforce completo appaiano nella sezione Recenti. Per velocizzare l'inserimento degli oggetti nella sezione Recenti è possibile bloccare gli oggetti dalla schermata dei risultati di ricerca nel sito completo. |
| Operazioni | L'elenco delle operazioni aperte e chiuse di un utente, e le operazioni che sono state delegate. |
| Today | App che consente agli utenti di pianificare e gestire la loro giornata integrando gli eventi del calendario del dispositivo mobile con le operazioni, gli account e i referenti di Salesforce associati. L'app consente inoltre agli utenti di entrare rapidamente nelle teleconferenze, registrare velocemente note sugli eventi e molto altro. Disponibile solo nelle app scaricabili Salesforce1. |
| Schede delle pagine Visualforce | Solo le pagine Visualforce per cui è stata selezionata la casella di controllo `Disponibile per le applicazioni mobili Salesforce` verranno visualizzate in Salesforce1. |

## Aspetti da tenere presenti

- Non è possibile impostare configurazioni diverse del menu per tipi diversi di utenti.
- Tutti gli elementi rappresentati da una scheda in Salesforce (oggetti standard e personalizzati, pagine Visualforce, feed, persone o gruppi) sono visibili nel menu di Salesforce1 a seconda delle impostazioni del profilo utente. Ad esempio, un utente assegnato a un profilo che ha la scheda Gruppi impostata su Scheda nascosta non vedrà la voce di menu Gruppi in Salesforce1, anche se questa è stata inclusa nel menu da un amministratore.
- Il menu di navigazione di una comunità non viene controllato tramite la pagina di impostazioni del Menu di navigazione. il cui contenuto è determinato dalle schede specificate in Schede e pagine nelle impostazioni di amministrazione della comunità.

VEDERE ANCHE:

Personalizzazione del menu di navigazione di Salesforce1

Note sul menu di navigazione di Salesforce1

Abilitazione delle pagine Visualforce per l'uso nell'app mobile Salesforce1

## Personalizzazione del menu di navigazione di Salesforce1

Personalizzare l'uso di Salesforce sui dispositivi mobili per gli utenti selezionando voci di menu, app, pagine Visualforce o Pagine Lightning da visualizzare nel menu di navigazione di Salesforce1.

> Nota: per poter includere pagine Visualforce, pagine Lightning o componenti Lightning nel menu di navigazione di Salesforce1, è necessario prima creare le relative schede. Da Imposta, immettere *Schede* nella casella `Ricerca veloce`, quindi selezionare **Schede**.

Consulta la guida passo passo: Personalizzazione del menu di navigazione di Salesforce1

1. Da Imposta, immettere *Navigazione in Salesforce1* nella casella `Ricerca veloce`, quindi selezionare **Navigazione in Salesforce1**.
2. Selezionare le voci dall'elenco Disponibile e fare clic su **Aggiungi**.

EDIZIONI

Disponibile in Lightning Experience nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Disponibile in Salesforce Classic in: **tutte** le versioni tranne Database.com Edition

AUTORIZZAZIONI UTENTE

Per personalizzare il menu di navigazione di Salesforce1:

- "Personalizza applicazione"

3. Per ordinare le voci, selezionarle una a una e fare clic su **Su** o **Giù**.

   L'ordine in cui le voci del menu vengono riportate nell'elenco Selezionati è l'ordine in cui vengono visualizzate nel menu di navigazione.

   > Nota: La prima voce dell'elenco Selezionati diventa la landing page di Salesforce1.

4. Fare clic su **Salva**.

Una volta salvate, le voci del menu di navigazione dovrebbero apparire nell'ordine corretto in Salesforce1. Può essere necessario aggiornare la pagina per vedere le modifiche.

**Suggerimento:** Quando si organizzano le voci di menu, posizionare all'inizio dell'elenco quelle preferite dagli utenti. La voce Elementi di ricerca intelligente si può espandere in una serie di otto o più voci di menu e potrebbe spingere altri elementi al di sotto del punto di scorrimento se è posizionata in alto nel menu. Qualsiasi voce posizionata sotto Elementi di ricerca intelligente appare nella sezione App del menu di navigazione.

VEDERE ANCHE:

Menu di navigazione dell'app mobile Salesforce1

Note sul menu di navigazione di Salesforce1

Abilitazione delle pagine Visualforce per l'uso nell'app mobile Salesforce1

## Note sul menu di navigazione di Salesforce1

EDIZIONI

Disponibile in Lightning Experience nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Disponibile in Salesforce Classic in: **tutte** le versioni tranne Database.com Edition

Pur essendo stati utilizzati di recente, alcuni oggetti non vengono inseriti nel menu di navigazione di Salesforce1.

- Operazioni ed eventi
- Persone, gruppi e cruscotti digitali, se questi elementi sono stati aggiunti direttamente al menu di navigazione
- Visualizzazioni elenco, che compaiono solo nelle pagine iniziali degli oggetti e non nel menu di navigazione
- Oggetti non disponibili in Salesforce1, compresi gli oggetti che non dispongono di una scheda nel sito completo di Salesforce.

### Voci di menu Cruscotti digitali, Persone e Gruppi

Se le voci di menu Cruscotti digitali, Persone o Gruppi non si aggiungono all'elenco Selezionati per il menu di navigazione, esse vengono inserite automaticamente nel gruppo di oggetti Elementi di ricerca intelligente e compaiono nella sezione Recenti del menu in Salesforce1. Se i Cruscotti digitali, le Persone o i Gruppi vengono aggiunti singolarmente all'elenco Selezionati per il menu di navigazione, essi compaiono al di fuori della sezione Recenti e la loro posizione nel menu di Salesforce1 si può personalizzare esattamente come le Operazioni, Today e le altre singole voci di menu.

### Blocco di un oggetto nella sezione Recenti

Gli utenti possono personalizzare gli oggetti che compaiono nella sezione Recenti del menu di navigazione Salesforce1. Se cercano un oggetto nel sito completo, possono passare il mouse sopra il nome dell'oggetto e fare clic su per bloccarlo in cima ai risultati della ricerca. L'ordine degli oggetti bloccati nel sito completo determina l'ordine degli oggetti che restano bloccati in cima alla sezione Recenti del menu di navigazione. Tuttavia, se si bloccano gli oggetti in questo modo, gli oggetti non bloccati che restano nella sezione Recenti finiscono dietro all'elemento **Altro**.

VEDERE ANCHE:

Menu di navigazione dell'app mobile Salesforce1

Personalizzazione del menu di navigazione di Salesforce1

# Notifiche dell'app mobile Salesforce1

EDIZIONI

Salesforce1 disponibile in: **tutte** le versioni tranne Database.com Edition

Le notifiche consentono agli utenti di sapere quando si verificano determinati eventi in Salesforce. Ad esempio, le notifiche consentono agli utenti di sapere quando ricevono le richieste di approvazione o quando qualcuno li menziona in Chatter.

Gli utenti di Salesforce1 possono visualizzare due tipi di notifiche.

- *Le notifiche all'interno delle applicazioni* (in-app) tengono aggiornati gli utenti sulle attività che li riguardano quando utilizzano Salesforce1. Toccando l'icona , un utente può visualizzare le 20 notifiche più recenti ricevute negli ultimi 90 giorni.

  Se Comunità Salesforce è abilitata per l'organizzazione, gli utenti visualizzano le notifiche di tutte le comunità di cui sono membri. Per aiutare gli utenti a identificare facilmente da quale comunità proviene una notifica, il nome della comunità è visualizzato dopo l'indicazione oraria.

- Le *notifiche push* sono avvisi visualizzati su un dispositivo mobile quando un utente ha installato l'app scaricabile di Salesforce1 ma non la sta utilizzando. Possono essere costituite da testo, icone e suoni, in base al tipo di dispositivo. Se un amministratore abilita le notifiche push per l'organizzazione, i singoli utenti possono scegliere se riceverle sui propri dispositivi.

Nota: Alcune notifiche contengono il testo inserito dagli utenti in Salesforce. Per garantire che non vengano distribuite informazioni riservate tramite un servizio di terzi senza la dovuta autorizzazione, le notifiche push contengono informazioni limitate (ad esempio un nome utente) a meno che non sia stata abilitata l'inclusione del contenuto completo nelle notifiche push.

Ad esempio, si supponga una notifica all'interno dell'applicazione con il seguente testo: "Lucia Renzi ti ha menzionato: @Mario Rossi, attenzione! Nuova strategia di vendita per account Acme." Per impostazione predefinita, il testo della notifica push equivalente sarebbe "Lucia Renzi ti ha menzionato". Tuttavia, se è stato abilitato il contenuto completo nelle notifiche push, questa notifica push includerà lo stesso contenuto (completo) della notifica all'interno dell'applicazione.

## Termini e condizioni per l'inclusione di contenuto completo nelle notifiche push

Se si accede alla pagina Impostazioni notifiche sul sito completo e si seleziona l'opzione per l'inclusione del contenuto completo nelle notifiche push, viene visualizzata una finestra popup con i termini e le condizioni. Fare clic su **OK** nella finestra popup per accettare questi termini e condizioni per conto della propria società.

**Notifiche Salesforce 1 Push Mobile**

La funzione di notifica push del contenuto completo di Salesforce1 fornisce agli utenti dell'organizzazione (collettivamente "gli utenti") aggiornamenti in tempo reale, ad esempio ogni volta che ricevono una menzione in un post o una richiesta di approvazione. La frequenza delle notifiche inviate dipenderà dal numero delle azioni che riguardano l'utente.

Per abilitare o disabilitare le notifiche push del contenuto completo in qualsiasi momento, da Imposta immettere `Impostazioni notifiche` nella casella `Ricerca veloce`, selezionare **Impostazioni notifiche**, quindi selezionare o deselezionare "Includi il contenuto completo nelle notifiche push".

Per gli utenti dell'organizzazione con dispositivi mobili su piattaforma iOS, l'uso della funzione di notifica push del contenuto completo determina la trasmissione dei dati contenuti nelle notifiche (compresi, potenzialmente, dati di clienti e/o informazioni riservate, secondo la definizione di questi termini presente nell'accordo di fornitura di servizi che disciplina l'utilizzo dei prodotti Salesforce) ad Apple Inc. e alle entità affiliate (collettivamente, "Apple"). Salesforce non sarà responsabile per la riservatezza, la sicurezza o l'integrità dei dati eventualmente trasmessi ad Apple.

Se si è autorizzati ad abilitare questa funzionalità e ad accettare queste condizioni dalla società che ha acquistato gli abbonamenti associati all'uso dei servizi Salesforce, confermare l'accettazione selezionando la casella "OK" qui sotto. Se non si è autorizzati dalla società di cui sopra ad accettare queste condizioni e ad abilitare questa funzionalità, fare clic su "Annulla".

VEDERE ANCHE:

Abilitazione delle notifiche dell'app mobile Salesforce1

## Abilitazione delle notifiche dell'app mobile Salesforce1

Consentire a tutti gli utenti dell'organizzazione di ricevere notifiche mobili in merito a eventi in Salesforce, ad esempio quando ricevono richieste di approvazione o quando qualcuno li menziona in Chatter.

1. Da Imposta, immettere *Notifiche di Salesforce1* nella casella `Ricerca veloce`, quindi selezionare **Notifiche di Salesforce1**.
2. Selezionare le notifiche che dovranno ricevere gli utenti di Salesforce1.
3. Se si è autorizzati a compiere questa azione per la propria società, selezionare `Includi il contenuto completo nelle notifiche push`.
4. Fare clic su **Salva**. Se è stata contrassegnata la casella di controllo per l'inclusione del contenuto completo nelle notifiche push, viene visualizzata una finestra popup contenente i termini e le condizioni. Fare clic su **OK** o su **Annulla**.

   Abilitando questa opzione, si esprime l'accettazione dei termini e delle condizioni per conto della propria società. Per i dettagli, vedere Notifiche dell'app mobile Salesforce1 a pagina 695.

Un utente può ricevere richieste di approvazione nelle notifiche di Salesforce1 solo quando riceve richieste di approvazione sotto forma di notifiche email. L'amministratore o l'utente può modificare il campo utente `Ricevi messaggi email con richiesta di approvazione` per impostare questa preferenza.

VEDERE ANCHE:

Notifiche dell'app mobile Salesforce1

EDIZIONI

Disponibile in Lightning Experience nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Disponibile in Salesforce Classic in: **tutte** le versioni tranne Database.com Edition

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni di notifica:

- "Visualizza impostazione e configurazione"

Per modificare le impostazioni di notifica:

- “Personalizza applicazione”

# Accesso offline all'app mobile Salesforce1

EDIZIONI

Disponibile in Lightning Experience nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Disponibile in Salesforce Classic in: **tutte** le versioni tranne Database.com Edition

Salesforce1 può memorizzare nella cache i dati a cui si è avuto accesso recentemente, in modo che siano disponibili quando il dispositivo di un utente è offline oppure non può essere connesso a Salesforce. L'accesso offline è attualmente di sola lettura ed è disponibile nelle app scaricabili di Salesforce1 per i dispositivi iOS e Android.

L'accesso offline viene abilitato la prima volta che un utente dell'organizzazione installa una delle app scaricabili di Salesforce1. Questa impostazione può essere gestita dalla pagina Salesforce1 Offline in Imposta.

Con l'accesso offline attivato, l'app esegue automaticamente la cache dei record degli oggetti elencati nella sezione Recenti del menu di navigazione di Salesforce1 a cui l'utente ha avuto accesso più di recente e dei cruscotti digitali recenti dell'utente. I record a cui l'utente ha avuto accesso di recente vengono determinati in base alle attività di un utente sia nell'app mobile sia nel sito Salesforce completo. Inoltre, l'app esegue la cache di molti dei dati a cui un utente accede nel corso di una sessione in Salesforce1.

I dati inseriti nella cache vengono crittografati e memorizzati in un archivio dati protetto e permanente.

Nella tabella che segue sono indicati i dati e gli elementi di Salesforce1 disponibili offline.

| Elemento di Salesforce1 | Disponibile per l'utilizzo offline |
|---|---|
| Menu di navigazione | Sì |
| Ricerca globale | Solo ricerche precedenti |
| Notifiche | Solo quelli già visualizzati |
| Feed, Gruppi e Persone | Solo quelli già visualizzati |
| Salesforce Today | Pagina principale e record di eventi mobili se visualizzati in precedenza |
| Eventi di Salesforce | Solo quelli già visualizzati |
| Oggetti recenti | Sì (i primi cinque) |
| Altri oggetti | No |
| Dettagli record | Sì (i 30 record più recenti) |
| Record correlati | Solo quelli già visualizzati |
| Visualizzazioni elenco | Solo quelli già visualizzati |
| Operazioni | Solo le operazioni della prima pagina dell'elenco Operazioni personali (fino a 10 operazioni) e solo se l'elenco è stato visualizzato in precedenza o dopo che l'utente ha aggiornato manualmente la cache |
| Cruscotti digitali | Sì (i primi cinque) |
| Approvazioni (invio, approvazione o rifiuto) | No |
| Pagine Visualforce | No |

| Elemento di Salesforce1 | Disponibile per l'utilizzo offline |
|---|---|
| App dell'area di disegno | No |
| Pagine Lightning | No |
| Impostazioni | Sì |

I dati inseriti nella cache vengono aggiornati quando un utente passa a Salesforce1. Se un utente passa a un'altra app, i suoi dati memorizzati nella cache vengono automaticamente aggiornati se l'archivio dati esiste da più di un'ora.

Gli utenti possono inserire manualmente i loro dati nella cache in qualsiasi momento, ad esempio prima di accedere alla modalità aereo o in un'area senza servizi. Dal menu di navigazione di Salesforce1, selezionare **Impostazioni** > **Cache offline** > **Esegui cache ora**.

Nota: La cache viene salvata per due settimane. Gli utenti possono svuotare la cache effettuando la disconnessione dall'app Salesforce1.

# Abilitazione delle pagine Visualforce per l'uso nell'app mobile Salesforce1

È possibile utilizzare Visualforce per estendere l'app Salesforce1 e fornire agli utenti mobili le funzionalità di cui hanno bisogno quando lavorano fuori ufficio. Prima di aggiungere una pagina Visualforce a Salesforce1, assicurarsi che la pagina sia abilitata per l'uso su dispositivi mobili altrimenti non sarà disponibile nelle app mobili.

Suggerimento: Prima di esporre le pagine Visualforce esistenti in Salesforce1, valutare in che modo appariranno e funzioneranno su telefoni cellulari e tablet. Probabilmente sarà necessario creare una nuova pagina realizzata specificamente per i fattori di forma dei dispositivi mobili.

Le pagine Visualforce devono essere abilitate per l'uso sui dispositivi mobili perché possano essere visualizzate in queste aree dell'interfaccia utente di Salesforce1:

- Il menu di navigazione, tramite una scheda Visualforce
- La barra delle azioni, tramite un'azione personalizzata
- Schede mobili sulla pagina delle informazioni correlate a un record
- Pulsanti standard sostituiti o pulsanti e link personalizzati
- Incorporate nei layout delle pagine dei dettagli del record
- Pagine Lightning

Per abilitare una pagina Visualforce per Salesforce1:

1. Da Imposta, immettere *`Pagine Visualforce`* nella casella `Ricerca veloce`, quindi selezionare **Pagine Visualforce**.
2. Fare clic su **Modifica** per la pagina Visualforce desiderata.
3. Selezionare `Disponibile per le applicazioni mobili Salesforce e per le pagine Lightning`, quindi fare clic su **Salva**.

Tenere presenti queste note sul supporto di Visualforce in Salesforce1.

- Le schede standard, le schede degli oggetti personalizzati e le visualizzazioni elenco sostituite da una pagina Visualforce non sono supportate in Salesforce1. La pagina Visualforce viene visualizzata per gli utenti del sito completo ma gli utenti di Salesforce1 vedranno la pagina predefinita di Salesforce1 per l'oggetto. Questa limitazione esiste per mantenere l'uso di Salesforce1 per gli oggetti.
- Inoltre è possibile abilitare le pagine Visualforce per Salesforce1 mediante l'API dei metadati, modificando il campo `isAvailableInTouch` nell'oggetto ApexPage.
- La casella di controllo `Pronto per Salesforce Classic mobile` nelle pagine di impostazione della Scheda Visualforce riguarda esclusivamente Salesforce Classic mobile e non ha alcun effetto sulle pagine Visualforce delle app Salesforce1.

EDIZIONI

Disponibile in Lightning Experience nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Disponibile in Salesforce Classic in: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per abilitare la visualizzazione di Visualforce in Salesforce1:

- "Personalizza applicazione"

  "Apex autore"

VEDERE ANCHE:

Personalizzazione del menu di navigazione di Salesforce1

## Immagine aziendale personalizzata per l'applicazione mobile Salesforce1

È possibile personalizzare l'applicazione mobile Salesforce1 in modo che sia in linea con l'aspetto e la grafica della propria immagine aziendale per renderla immediatamente riconoscibile ai propri utenti mobili. L'immagine aziendale personalizzata viene visualizzata in tutte le applicazioni mobili Salesforce1.

EDIZIONI

Disponibile in Lightning Experience nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Disponibile in Salesforce Classic in: **tutte** le versioni tranne Database.com Edition

Nota: Le immagini caricate per personalizzare l'app Salesforce1 sono archiviate in una cartella Documenti denominata Risorse per immagine aziendale Salesforce1. Per questo motivo, è necessario abilitare l'oggetto Documenti per la propria organizzazione prima che gli amministratori possano visualizzare e modificare la pagina Immagine aziendale di Salesforce1 (tuttavia, non è necessario che la scheda Documenti sia visibile).

Per consentire agli utenti dell'app browser mobile Salesforce1 di visualizzare l'immagine aziendale personalizzata, è necessario che per la propria organizzazione siano abilitati i Documenti. Per gli utenti delle app scaricabili di Salesforce1, gli utenti devono inoltre disporre delle autorizzazioni utente "Lettura" per i Documenti.

È possibile personalizzare:

| Elemento | Descrizione |
| --- | --- |
| Colore elementi immagine aziendale | Il colore degli elementi principali dell'interfaccia utente, quali intestazione, pulsanti e barra di ricerca.<br>In base al colore scelto, i colori di contrasto per gli elementi dell'interfaccia utente quali i bordi del menu di navigazione, l'elenco delle notifiche e il testo dei pulsanti, vengono definiti automaticamente.<br>Le intestazioni su sovrapposizioni, finestre popup e di dialogo, ad esempio le finestre di modifica e creazione o le finestre che si aprono a partire dalle azioni nella barra delle azioni, non sono interessate da questa impostazione. Queste intestazioni sono sempre bianche, per fornire un'indicazione visiva del fatto che l'utente sta eseguendo una modifica e non semplicemente visualizzando delle informazioni. |
| Colore pagina di caricamento | Il colore di sfondo della pagina di caricamento che viene visualizzata all'accesso di un utente mobile. |
| Logo pagina di caricamento | L'immagine nella pagina di caricamento che viene visualizzata all'accesso di un utente mobile.<br>Per un risultato migliore si consiglia di utilizzare un'immagine alla massima dimensione consentita. Le dimensioni massime sono 460 pixel per 560 pixel. |

Prendere in considerazione i seguenti suggerimenti al momento di personalizzazione l'immagine aziendale per l'app Salesforce1:

- Durante la creazione dell'immagine del logo, assicurarsi di comprimerla. In molti programmi per la modifica delle immagini, questo processo viene definito con termini come "usa compressione", "ottimizza immagine", "salva per il Web" o "riduci per il Web".
- Verificare che il logo venga visualizzato correttamente in Salesforce1, utilizzando gli stessi dispositivi della propria base di utenti e non solo il monitor di un computer desktop. L'immagine può comparire in diverse scale o proporzioni a seconda delle dimensioni dello schermo e della densità di pixel di ogni dispositivo.
- Salesforce1 supporta i formati immagine `.png`, `.gif` e `.jpg` per gli elementi immagine aziendale personalizzati, ma per ottenere i migliori risultati si consiglia di utilizzare il formato .png.

- Questi elementi dell'interfaccia non possono essere personalizzati:
  - L'icona dell'app Salesforce1 che appare sulla schermata iniziale del dispositivo mobile.
  - La schermata di caricamento inziale quando si lancia l'app scaricabile Salesforce1 per iOS. Questa schermata di caricamento viene visualizzata prima che l'utente arrivi alla pagina di accesso.
- Per vedere eventuali modifiche all'immagine aziendale personalizzata, gli utenti mobili devono chiudere l'applicazione ed effettuare nuovamente l'accesso.

È anche possibile personalizzare l'immagine aziendale della pagina di accesso dell'app Salesforce1. Per modificare la pagina di accesso è necessario che Dominio personale sia abilitato. Per personalizzare la pagina di accesso Salesforce1 della propria azienda, vedere Personalizzazione dell'immagine aziendale della pagina di accesso a pagina 539.

VEDERE ANCHE:

Modifica dell'immagine aziendale dell'app mobile Salesforce1 per l'organizzazione

## Modifica dell'immagine aziendale dell'app mobile Salesforce1 per l'organizzazione

EDIZIONI

Disponibile in Lightning Experience nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

Disponibile in Salesforce Classic in: **tutte** le versioni tranne Database.com Edition

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni dell'immagine aziendale di Salesforce1:

- "Visualizza impostazione e configurazione"

Per modificare le impostazioni dell'immagine aziendale di Salesforce1:

- "Personalizza applicazione"

  "Modifica tutti i dati"

Per l'app mobile Salesforce1 è possibile modificare il colore di sfondo e il logo della pagina di caricamento, nonché il colore di sfondo dell'intestazione, in modo che siano in linea con l'immagine della propria azienda.

Nota: Le immagini caricate per personalizzare l'app Salesforce1 sono archiviate in una cartella Documenti denominata Risorse per immagine aziendale Salesforce1. Per questo motivo, è necessario abilitare l'oggetto Documenti per la propria organizzazione prima che gli amministratori possano visualizzare e modificare la pagina Immagine aziendale di Salesforce1. (Tuttavia, non è necessario che la scheda Documenti sia visibile).

Per consentire agli utenti dell'app browser mobile Salesforce1 di visualizzare l'immagine aziendale personalizzata, è necessario che per la propria organizzazione siano abilitati i Documenti. Per gli utenti delle app scaricabili di Salesforce1, gli utenti devono inoltre disporre delle autorizzazioni utente "Lettura" per i Documenti.

1. Da Imposta, immettere `Immagine aziendale` nella casella `Ricerca veloce`, quindi selezionare **Immagine aziendale Salesforce1** e fare clic su **Modifica**.
2. Per personalizzare il colore degli elementi principali dell'interfaccia utente, tra cui l'intestazione, fare clic su oppure inserire un codice colore esadecimale valido.
3. Per personalizzare il colore di sfondo della pagina di caricamento, fare clic su o immettere un codice colore esadecimale valido.
4. Per personalizzare il logo della pagina di caricamento, fare clic su **Scegli file** per caricare un'immagine. Le immagini possono essere file .jpg, .gif o .png di dimensioni fino a 200 KB. Le dimensioni massime sono 460 pixel per 560 pixel.
5. Fare clic su **Salva**.

VEDERE ANCHE:

Immagine aziendale personalizzata per l'applicazione mobile Salesforce1

# SalesforceA

Gestione degli utenti e visualizzazione delle informazioni delle organizzazioni Salesforce dal dispositivo mobile.

SalesforceA è un'applicazione per dispositivi mobili destinata agli amministratori Salesforce. Quando si è lontani dalla propria scrivania, è possibile utilizzare il telefono o il tablet per eseguire operazioni di amministrazione essenziali come la reimpostazione delle password, l'assegnazione di insiemi di autorizzazioni e la visualizzazione dello stato attuale del sistema.

SalesforceA è gratuito e può essere scaricato da Google Play Store per i telefoni e tablet Android e da Apple App Store per Apple iPhone, iPod Touch e iPad.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**.

AUTORIZZAZIONI UTENTE

Per utilizzare SalesforceA:

- "Gestisci utenti"

**Panoramica dell'organizzazione**

La schermata Panoramica indica:

- Numero di utenti bloccati
- Prossima manutenzione programmata

L'icona di navigazione è in alto a sinistra, toccarla per passare al menu di navigazione.

**Gestione degli utenti**

Dal menu di navigazione, toccare **Utenti** per visualizzare un elenco di utenti o cercare un utente. Toccare un nome per:

- Visualizzare o modificare i dettagli dell'utente
- Bloccare, disattivare o riattivare l'utente
- Reimpostare la password di un utente
- Assegnare insiemi di autorizzazioni

Scorrere fino alla pagina Correlato per visualizzare:

- L'attuale insieme di autorizzazioni dell'utente
- La cronologia degli accessi dell'utente

**Informazioni aggiuntive**

Il menu di navigazione fornisce l'accesso rapido anche a:

- Salesforce Success Community
- note di rilascio di Salesforce
- stato del sistema

IN QUESTA SEZIONE:

Accesso a SalesforceA

Accedere all'applicazione mobile SalesforceA per eseguire operazioni amministrative essenziali per l'organizzazione Salesforce.

Accesso a più organizzazioni con SalesforceA

Utilizzare SalesforceA sul dispositivo mobile per accedere a più organizzazioni Salesforce di cui si è amministratori. Eseguito l'accesso, è possibile passare da un'organizzazione all'altra senza ripetere la procedura di accesso.

VEDERE ANCHE:

Accesso a SalesforceA

Accesso a più organizzazioni con SalesforceA

## Accesso a SalesforceA

Accedere all'applicazione mobile SalesforceA per eseguire operazioni amministrative essenziali per l'organizzazione Salesforce.

L'amministratore Salesforce può utilizzare SalesforceA per accedere all'organizzazione di produzione (impostazione predefinita), all'ambiente Sandbox o a un host personalizzato. Scegliere l'ambiente o l'host con il menu dell'host.

- Per gli utenti iOS: aprire il menu dell'host dall'icona a forma di ingranaggio nell'angolo superiore destro della schermata di accesso.
- Per gli utenti Android: aprire il menu dell'host dal pulsante del menu del dispositivo.

Se richiesto, immettere un codice di accesso come ulteriore livello di protezione per il dispositivo mobile. Questa impostazione di protezione può essere gestita nell'applicazione browser desktop Salesforce da **Imposta**, nella voce **Applicazioni connesse** per **SalesforceA**.

Una volta eseguito l'accesso, viene visualizzata la schermata Panoramica. L'icona di navigazione è in alto a sinistra.

VEDERE ANCHE:

SalesforceA

Accesso a più organizzazioni con SalesforceA

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**.

AUTORIZZAZIONI UTENTE

Per utilizzare SalesforceA:

- "Gestisci utenti"

## Accesso a più organizzazioni con SalesforceA

Utilizzare SalesforceA sul dispositivo mobile per accedere a più organizzazioni Salesforce di cui si è amministratori. Eseguito l'accesso, è possibile passare da un'organizzazione all'altra senza ripetere la procedura di accesso.

1. Toccare l'icona di navigazione per accedere al menu.
2. Toccare la freccia giù accanto al nome utente. Viene visualizzato un elenco di tutti gli account.
3. Toccare **+ Aggiungi account**. Per scegliere un Sandbox o un host personalizzato, toccare l'icona a forma di ingranaggio in alto a destra (utenti iOS) o il pulsante del menu del dispositivo (utenti Android) e passare all'host desiderato.
4. Selezionare un nome utente salvato in precedenza o toccare **Accedi con un nome utente diverso** per aggiungere un account.

Dall'elenco degli account è possibile:

- Passare da un'organizzazione a un'altra
- Vedere se ciascuna organizzazione è di produzione o Sandbox
- Vedere la versione di ogni organizzazione

Toccare la freccia su per tornare al menu di navigazione.

VEDERE ANCHE:

SalesforceA

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Contact Manager Edition**, **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**.

AUTORIZZAZIONI UTENTE

Per utilizzare SalesforceA:

- "Gestisci utenti"

# Salesforce Classic

## Panoramica su Salesforce Classic mobile per gli amministratori

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

Salesforce Classic mobile facilita l'attività dei team mobili consentendo loro di accedere ai dati Salesforce più recenti dovunque si trovino e in qualsiasi momento, direttamente da dispositivi di tipo Android™, BlackBerry® e iPhone®. L'applicazione Salesforce Classic mobile scambia dati con Salesforce tramite rete wireless o mobile e memorizza una copia locale dei dati dell'utente in un proprio database sul dispositivo mobile. Quando non è disponibile una connessione dati, gli utenti possono modificare le copie locali dei rispettivi record di Salesforce e trasmettere tali modifiche a Salesforce quando la connessione è nuovamente disponibile. L'applicazione favorisce inoltre la registrazione quasi in tempo reale delle informazioni critiche, chiedendo agli utenti di inserire gli aggiornamenti direttamente in Salesforce o nelle applicazioni Force.com AppExchange dopo telefonate, email o appuntamenti importanti con i clienti.

Per utilizzare la versione completa di Salesforce Classic mobile è necessario disporre della relativa licenza per ogni singolo utente. Per le organizzazioni che utilizzano le versioni Unlimited Edition, Performance Edition e Developer Edition, Salesforce fornisce una licenza Salesforce Mobile per ogni licenza Salesforce. Le organizzazioni che utilizzano la versione Professional Edition o Enterprise Edition devono invece acquistare le licenze mobili separatamente.

Gli utenti Salesforce che non dispongono di una licenza mobile possono scaricare una versione gratuita e limitata di Salesforce Classic mobile. La versione gratuita:

- Supporta meno oggetti standard
- Non supporta gli oggetti personalizzati
- Non consente agli amministratori di personalizzare o creare configurazioni mobili
- Non è disponibile per essere utilizzata dagli utenti del Portale partner

Nota: Le app per Android, BlackBerry e iPhone sono disponibili in inglese, giapponese, francese, tedesco e spagnolo. Contattare Salesforce per attivare Salesforce Classic mobile per l'organizzazione.

VEDERE ANCHE:

Impostazione di Salesforce Classic mobile

## Informazioni sulla configurazione Salesforce Classic mobile predefinita

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

Le configurazioni mobili per l'applicazione Salesforce Classic mobile sono serie di parametri che determinano quali dati vengono trasmessi da Salesforce ai dispositivi mobili degli utenti nonché quali utenti ricevono tali dati sui propri dispositivi mobili. Per le organizzazioni Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition e Developer Edition, viene fornita una configurazione mobile predefinita. Gli amministratori non possono visualizzare né modificare la configurazione mobile predefinita.

Gli utenti vengono assegnati automaticamente alla configurazione mobile predefinita quando attivano il proprio account di Salesforce da un dispositivo mobile supportato mediante l'applicazione Salesforce Classic mobile.

La configurazione mobile predefinita:

- Consente agli utenti cui sia stata assegnata una licenza mobile di installare e attivare Salesforce Classic mobile, anche se non sono ancora stati assegnati a una configurazione mobile;
- Consente agli utenti cui non è stata assegnata una licenza mobile di installare e attivare la versione gratuita di Salesforce Classic mobile.

È possibile disabilitare Salesforce Classic mobile per impedire agli utenti di attivare l'applicazione Salesforce Classic mobile.

La configurazione predefinita può rendere mobili i seguenti oggetti:

- Account
- Asset
- Casi
- Referenti
- Cruscotti digitali
- Eventi
- Lead
- Opportunità
- Rapporti
- Soluzioni
- Operazioni

Nota:

- Non tutti gli oggetti disponibili nell'applicazione Salesforce Classic mobile vengono resi disponibili sui dispositivi mobili con la configurazione predefinita.
- Gli asset non sono disponibili come scheda nell'applicazione Salesforce Classic mobile ma vengono visualizzati come elenco correlato per account, casi e referenti.

La configurazione predefinita sincronizza automaticamente i record aperti di recente dall'utente in Salesforce nell'applicazione Salesforce Classic mobile. Gli utenti possono cercare record che non sono sincronizzati automaticamente; una volta che l'utente scarica un record, questo diventa parte permanente della serie di dati. Oltre ai record richiamati di recente, la configurazione predefinita sincronizza le attività chiuse negli ultimi cinque giorni e le attività aperte da chiudere nei 30 giorni successivi.

# Suggerimenti e procedure consigliate per l'implementazione di Salesforce Classic mobile

Configurare l'applicazione Salesforce Classic mobile utilizzando i seguenti suggerimenti e procedure consigliate.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le configurazioni di Salesforce Classic mobile:

- "Visualizza impostazione e configurazione"

Per creare, modificare o eliminare configurazioni di Salesforce Classic mobile:

- "Gestisci configurazioni mobili"

## Creazione di serie di dati di piccole dimensioni

- Limitare al massimo il volume delle serie di dati nelle configurazioni mobili. Le serie di dati di piccole dimensioni non si limitano a migliorare notevolmente le prestazioni dell'applicazione Salesforce Classic mobile, ma semplificano anche l'uso dell'applicazione. Inviare grandi quantità di dati al dispositivo può sembrare una buona idea, ma i record importanti tendono a perdersi in mezzo a quelli che non sono rilevanti per le attività quotidiane degli utenti. Le serie di dati di piccole dimensioni sono più efficaci perché l'applicazione Salesforce Classic mobile si sincronizza con Salesforce ogni 20 minuti e quindi i dati vengono costantemente aggiornati in base ai record più recenti. Anche se le configurazioni mobili non prevedono ogni possibile record di cui gli utenti potrebbero necessitare, questi avranno la possibilità di cercare i record che non vengono sincronizzati automaticamente sui loro dispositivi.

  Per creare serie di dati di piccole dimensioni:

  - Nidificare gli oggetti nella struttura della serie di dati. Ad esempio, aggiungere i referenti come serie di dati secondaria dell'oggetto account per far sì che la serie di dati includa i referenti correlati agli account resi disponibili su dispositivi mobili anziché tutti i referenti dell'utente.
  - Evitare di impostare il filtro di proprietà dei record su Tutti i record a meno che l'organizzazione non utilizzi un modello di condivisione privato. È poco probabile che gli utenti abbiano bisogno di visualizzare tutti i record di un oggetto sui rispettivi dispositivi. Ad esempio, anziché rendere mobili tutti i record opportunità, rendere mobili solo le opportunità di cui è titolare l'utente o il relativo team opportunità.
  - Utilizzare filtri che sincronizzino i record più rilevanti. Ad esempio, anche se sul dispositivo si limitano le opportunità ai record di cui l'utente è titolare, è possibile sfrondare ulteriormente la serie di dati rendendo mobili solo le opportunità che si concludono in un determinato mese.
  - Impostare un limite per i record per evitare che la serie di dati diventi troppo grande. In genere, una singola serie di dati non dovrebbe generare più di 2.500 record.

- Un altro modo per creare serie di dati di piccole dimensioni consiste nel rendere mobile l'elenco delle voci recenti di Salesforce, aggiungere le serie di dati e impostare i filtri di proprietà dei record delle serie di dati su Nessuno (Solo ricerca). Alla serie di dati dell'utente vengono aggiunti i record consultati di recente in Salesforce e tali record a loro volta sincronizzano altri dati in base alla gerarchia della serie di dati. Si supponga ad esempio di creare una serie di dati con l'oggetto account al livello principale e di aggiungere l'oggetto referente, operazione ed evento come serie di dati secondarie. Quando sincronizza un account dall'elenco delle voci recenti di Salesforce, l'applicazione Salesforce Classic mobile sincronizza anche i referenti, le operazioni e gli eventi correlati a quell'account.
- In caso di dubbi su quali campi utilizzare come filtri per le serie di dati o le visualizzazioni mobili, prendere in considerazione l'utilizzo del campo Data ultima attività. Ad esempio, impostare un filtro che sincronizzi i referenti con un'attività registrata una determinata settimana o mese. Il campo Data ultima attività è un indicatore migliore della rilevanza di un record rispetto al campo Data ultima modifica: spesso i dettagli principali di un record restano invariati anche se gli utenti registrano spesso operazioni ed eventi correlati.

## Rendere mobili i record necessari agli utenti

- Prima di rendere mobile un oggetto personalizzato, verificare che le funzionalità dell'oggetto siano compatibili con l'applicazione Salesforce Classic mobile. Salesforce Classic mobile non supporta infatti gli S-Control, i mashup, i campi unione, i campi immagine o i link personalizzati.
- Per ottenere una serie di attività rilevanti, rendere mobili gli oggetti operazione ed evento al livello principale della gerarchia della serie di dati e nidificarli sotto oggetti principali quali referenti, account e opportunità. L'aggiunta di operazioni e di eventi a più livelli garantisce che gli utenti possano visualizzare le attività personali e quelle relative ai record presenti sui rispettivi dispositivi. Evitare di rendere mobile una quantità eccessiva di cronologia attività o di operazioni ed eventi di cui l'utente non è titolare. In genere in un'organizzazione i record operazione ed evento sono più numerosi di qualsiasi altro tipo di record e, pertanto, è facile gonfiare le serie di dati con troppe attività.
- Se i propri rappresentanti fanno spesso ordini sul campo e necessitano di un elenco completo delle giacenze, aggiungere l'oggetto prodotto al livello principale della gerarchia della serie di dati. Se si nidifica il prodotto opportunità sotto l'oggetto opportunità non verranno resi mobili tutti i prodotti.
- Se gli utenti devono assegnare delle operazioni ad altri utenti o modificare il titolare di un record, rendere mobile l'oggetto utente per rendere disponibili i nomi di altri utenti sul dispositivo. Evitare di rendere mobili tutti i record utente, ma impostare invece dei filtri basati sul ruolo o sul profilo.
- Verificare che gli utenti assegnati a una configurazione mobile dispongano dell'accesso a livello di campo a tutti i campi utilizzati nei criteri di filtro della configurazione. Se un utente non è autorizzato ad accedere a un campo presente nei criteri di filtro di una serie di dati, l'applicazione Salesforce Classic mobile non sincronizzerà i record di quella serie di dati o delle relative serie di dati secondarie.
- Per ovviare alle limitazioni dell'applicazione Salesforce Classic mobile, in alcuni casi è possibile utilizzare campi di formula oggetti incrociata. Ad esempio, Salesforce Classic mobile non supporta le campagne e quindi è impossibile aggiungere l'oggetto campagna come serie di dati e l'oggetto opportunità come serie di dati secondaria per richiamare i record correlati. Tuttavia, è possibile creare un campo formula testuale sull'oggetto opportunità uguale al nome della campagna controllante. Il campo deve essere visibile ma non deve essere necessariamente incluso nei layout di pagina. Aggiungere quindi l'oggetto opportunità alla serie di dati e utilizzare il nuovo campo formula per filtrare le opportunità relative a una campagna specifica.
- Sebbene una configurazione mobile possa includere un oggetto a più livelli gerarchici della serie di dati, gli utenti non visualizzeranno doppioni di schede nell'applicazione Salesforce Classic mobile. Il dispositivo visualizza infatti solo una scheda Operazione anche se si rende mobile l'oggetto operazione al livello principale e come serie di dati secondaria di tre oggetti.

## Personalizzazione delle configurazioni mobili

- Ripulire i layout di pagina mobili escludendo dei campi dagli oggetti nella configurazione mobile. Al dispositivo viene così inviata una minore quantità di dati, e gli utenti mobili non sono costretti a scorrere una serie di campi inutili.
- Se si rende mobile la scheda Cruscotti digitali, avere cura di selezionare tutte le altre schede che devono essere visualizzate nell'applicazione Salesforce Classic mobile. La personalizzazione delle schede di una configurazione mobile sostituisce il gruppo di schede predefinite: se si rende mobile solo la scheda Cruscotti digitali, questa sarà l'unica scheda inviata al dispositivo.
- A causa delle ridotte dimensioni dei display dei dispositivi mobili, è possibile selezionare solo due colonne per le visualizzazioni mobili. Se occorrono tre colonne di dati, creare un campo formula testuale sull'oggetto per concatenare i tre campi e quindi utilizzare il campo formula nei criteri della visualizzazione mobile.
- Durante la creazione delle visualizzazioni mobili, è possibile applicare un filtro basato sull'utente corrente con la variabile globale $User.ID, ma non è possibile immettere il nome di un utente come valore nei criteri di filtro. Per creare una visualizzazione basata sugli utenti, creare un campo formula testuale sull'oggetto appropriato, quindi utilizzare il campo formula nei criteri della visualizzazione mobile. Ad esempio, per creare una visualizzazione che mostra le opportunità di un team opportunità, creare un campo formula testuale sull'oggetto opportunità contenente l'ID utente o il ruolo del titolare opportunità, quindi creare una visualizzazione che applica un filtro in base ai valori del campo.

## Test e distribuzione dell'applicazione mobile

- È importante testare le configurazioni mobili per verificare che sincronizzino un volume accettabile di dati. Provare le configurazioni con degli utenti attivi titolari di grandi quantità di record. Solitamente, la maggior parte delle serie di dati genera un volume di dati compreso tra 500 KB e 4 MB. Se le serie di dati superano i 4 MB, restringere i criteri di filtro per limitare la quantità di dati inviata al dispositivo.
- L'applicazione Salesforce Classic mobile si può utilizzare nel Sandbox prima di distribuirla alla propria organizzazione.
- L'utilizzo dell'applicazione Salesforce Classic mobile necessita di un piano per i dati. Il volume dei dati wireless dell'applicazione Salesforce Classic mobile varia notevolmente da un cliente all'altro e persino da un utente all'altro nella stessa organizzazione. È impossibile prevedere l'utilizzo dei dati della propria organizzazione, ma esistono alcune linee guida:
  - Il download iniziale dei dati è rappresentato dai record che soddisfano i criteri specificati nella configurazione mobile dell'utente e dai metadati necessari per supportare tali record quando si è scollegati. In media, i volumi di dati sono compresi fra 500 KB e 4 MB.
  - Dopo il download iniziale dei dati, l'applicazione client richiede aggiornamenti incrementali ogni 20 minuti. Ciascuna di queste richieste e la relativa risposta del server ammontano a circa 200 byte.
  - Se in seguito alla richiesta di aggiornamento vengono scaricati dati nuovi nell'applicazione client, vengono inviati solo i valori nuovi o modificati. Ad esempio, l'applicazione Salesforce Classic mobile scarica solo il nuovo numero di telefono nel record di un referente, e non tutto il record. Il volume di dati trasmesso è diverso per ogni organizzazione e per ogni utente.

  Generalmente, il volume di dati trasmesso dall'applicazione Salesforce Classic mobile è ridotto rispetto a un utilizzo moderato dell'email.
- In caso di distribuzione agli utenti di BlackBerry, valutare l'infrastruttura di rete aziendale prima di implementare la soluzione mobile.

## Procedure consigliate

- Utilizzare l'opzione di implementazione senza amministrazione per fare esperimenti con l'applicazione Salesforce Classic mobile prima di impostare le configurazioni mobili. Dopo che si è provato a utilizzare l'applicazione Salesforce Classic mobile, si sarà in grado di creare modelli migliori per le configurazioni mobili.
- Chiedere agli utenti quali sono i rapporti, le visualizzazioni e i cruscotti digitali che prediligono per avere un'idea dei criteri di filtro da utilizzare nelle configurazioni mobili.
- Dopo avere impostato le configurazioni mobili, distribuire l'applicazione Salesforce Classic mobile su scala ridotta a un gruppo di utenti selezionati. Modificare le impostazioni dell'applicazione mobile in base al loro feedback e quindi distribuirla a tutti gli utenti.

## Impostazione di Salesforce Classic mobile

Per distribuire l'applicazione Salesforce Classic mobile all'organizzazione:

1. Rivedere i suggerimenti di implementazione mobile e le procedure consigliate
2. Abilitare gli utenti mobili
3. Creare una o più configurazioni mobili
4. Definire le serie di dati per le configurazioni mobili
5. Testare le configurazioni mobili
6. Personalizzare i layout di pagina mobili e mettere a punto le autorizzazioni degli utenti mobili (facoltativo)
7. Personalizzare le schede mobili (facoltativo)
8. Creare visualizzazioni personalizzate mobili (facoltativo)
9. Impostare i cruscotti digitali (facoltativo)
10. Impostare rapporti mobili (facoltativo)
11. Impostare Salesforce CRM Content (facoltativo)
12. Configurare l'accesso per gli utenti partner (facoltativo)
13. Creare link al Web e alle pagine Visualforce Mobile (facoltativo)
14. Avvisare gli utenti che Salesforce Classic mobile è disponibile per il download

Quando gli utenti scaricano l'applicazione Salesforce Classic mobile e attivano i propri account, è possibile gestire i loro dispositivi nella Console Amministrazione di Salesforce Classic mobile.

VEDERE ANCHE:

Gestione delle configurazioni di Salesforce Classic mobile

Gestione dei dispositivi di Salesforce Classic mobile

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni di Salesforce Classic mobile:

- "Visualizza impostazione e configurazione"

Per modificare le impostazioni di Salesforce Classic mobile:

- "Gestisci configurazioni mobili"

## Abilitazione degli utenti Salesforce Classic mobile

Per abilitare gli utenti ad accedere alla versione completa di Salesforce Classic mobile:

1. Assegnare le licenze mobili agli utenti selezionando la casella di controllo `Utente Salesforce Classic mobile` nel record dell'utente.
2. Modificare ogni profilo personalizzato a cui sono assegnati degli utenti Salesforce Classic mobile in modo da includere l'autorizzazione "API abilitata". Gli utenti Salesforce Classic mobile devono accedere all'API in modo che i loro dispositivi mobili possano comunicare con Salesforce. L'autorizzazione "API abilitata" è abilitata per impostazione predefinita sui profili standard.

Nota: Le app per Android, BlackBerry e iPhone sono disponibili in inglese, giapponese, francese, tedesco e spagnolo. Contattare Salesforce per attivare Salesforce Classic mobile per l'organizzazione.

Per evitare che gli utenti attivino la versione completa di Salesforce Classic mobile sui loro dispositivi mobili prima che l'organizzazione sia pronta a implementare l'applicazione, disabilitare la casella di controllo `Utente Salesforce Classic mobile` per tutti gli utenti.

Nota: Se si deseleziona questa casella di controllo per un utente già assegnato a una configurazione mobile, Salesforce rimuove tale utente dalla configurazione mobile e lo assegna alla configurazione mobile predefinita.

La versione gratuita di Salesforce Classic mobile è abilitata per impostazione predefinita. Se si desidera impedire che gli utenti che non dispongono di licenze Salesforce Classic mobile accedano ai propri dati Salesforce sui dispositivi mobili, disabilitare la versione gratuita di Salesforce Classic mobile.

1. Da Imposta, digitare *Impostazioni Salesforce Classic* nella casella `Ricerca veloce` e quindi selezionare **Impostazioni Salesforce Classic**.
2. Fare clic su **Modifica**.
3. Deselezionare `Abilitare Mobile Lite`.

   Nota: Se si deseleziona questa opzione mentre gli utenti eseguono l'applicazione Salesforce Classic mobile, i dati Salesforce presenti sui loro dispositivi verranno cancellati alla successiva sincronizzazione con Salesforce dei dispositivi.

4. Fare clic su **Salva**.

VEDERE ANCHE:

Impostazione di Salesforce Classic mobile

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni di Salesforce Classic mobile:

- "Visualizza impostazione e configurazione"

Per modificare le impostazioni di Salesforce Classic mobile:

- "Gestisci configurazioni mobili"

## Creazione di configurazioni di Salesforce Classic mobile

Le configurazioni mobili sono serie di parametri che determinano i dati che Salesforce trasmette ai dispositivi mobili degli utenti nonché quali utenti ricevono tali dati sui propri dispositivi mobili. Le organizzazioni possono creare più configurazioni mobili per soddisfare contemporaneamente le esigenze di vari tipi di utenti. Ad esempio, una configurazione mobile potrebbe inviare lead e opportunità alla divisione vendite e un'altra potrebbe inviare casi ai rappresentanti del servizio di assistenza clienti.

Prima di creare le configurazioni mobili, pianificare quali profili e utenti si desidera assegnare a ciascuna configurazione. Ogni configurazione mobile influisce solo sui dispositivi mobili degli utenti assegnati a essa.

Per creare una configurazione mobile:

1. Immissione delle informazioni di base
2. Assegnazione di utenti e profili
3. Impostazione del limite alle dimensioni totali dei dati
4. Completamento della configurazione mobile

Nota: Per le organizzazioni Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition e Developer Edition, viene fornita una configurazione mobile predefinita. La configurazione predefinita non può essere visualizzata né modificata.Gli utenti Salesforce che non dispongono di una licenza mobile possono scaricare una versione gratuita e limitata di Salesforce Classic mobile. Questi utenti vengono assegnati alla configurazione mobile predefinita quando attivano il proprio account di Salesforce da un dispositivo mobile.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le configurazioni di Salesforce Classic mobile:
- "Visualizza impostazione e configurazione"

Per creare, modificare o eliminare configurazioni di Salesforce Classic mobile:
- "Gestisci configurazioni mobili"

### Immissione delle informazioni di base

1. Da Imposta, immettere `Configurazioni Salesforce Classic` nella casella `Ricerca veloce`, quindi selezionare **Configurazioni Salesforce Classic** per accedere alla pagina con l'elenco delle configurazioni mobili.
2. Fare clic su **Nuova configurazione mobile**.
3. Immettere un nome per la configurazione mobile.
4. Se si desidera attivare la configurazione mobile subito dopo la sua creazione, selezionare la casella di controllo `Attivo`. La configurazione mobile non funziona se non si seleziona questa casella di controllo.

   Se si disattiva una configurazione mobile attiva, Salesforce salva tutte le richieste provenienti dai dispositivi degli utenti assegnati alla configurazione mobile per una settimana. Se si riattiva la configurazione mobile, Salesforce esegue le richieste nell'ordine in cui vengono ricevute.

5. Se lo si desidera, immettere una descrizione per la configurazione mobile.
6. Se lo si desidera, selezionare la casella di controllo `Rendi mobili voci recenti` per contrassegnare i record utilizzati di recente in Salesforce per la sincronizzazione dei dispositivi.

   La selezione di questa opzione garantisce che gli utenti mobili assegnati alla configurazione non siano costretti a cercare e scaricare elementi a cui hanno avuto recentemente accesso in Salesforce, anche se tali record non soddisfano i criteri di filtro della configurazione. Solo i record appartenenti agli oggetti resi disponibili su dispositivi mobili possono essere contrassegnati per la sincronizzazione dei dispositivi; ad esempio, se non si rende disponibile su dispositivi mobili l'oggetto account di una configurazione, gli utenti assegnati a tale configurazione non possono ricevere automaticamente gli account recenti sui loro dispositivi.

7. Se si seleziona la casella di controllo `Rendi mobili voci recenti`, selezionare un valore dall'elenco a discesa `Numero massimo di voci recenti`. Impostare un numero basso se gli utenti non dispongono di molto spazio libero sui loro dispositivi mobili.
8. Se lo si desidera, selezionare la casella di controllo `Rendi mobili i record seguiti` per sincronizzare automaticamente i record seguiti dagli utenti in Chatter con quelli dei loro dispositivi mobili. Il dispositivo sincronizza i record seguiti solo per gli oggetti inclusi nella serie di dati della configurazione mobile.

   La casella di controllo `Rendi mobili i record seguiti` è disponibile solo se per l'organizzazione è abilitato Chatter.

## Assegnazione di utenti e profili

È possibile assegnare singoli utenti e profili a ogni configurazione mobile. Se si assegna un profilo a una configurazione mobile, la configurazione mobile è valida per tutti gli utenti Salesforce Classic mobile con tale profilo, a meno che un utente specifico non sia assegnato a un'altra configurazione mobile.

Suggerimento: Per comodità di gestione, è consigliabile assegnare le configurazioni mobili ai profili; tuttavia, in alcune situazioni può essere necessario assegnare una configurazione direttamente ai singoli utenti.

Per assegnare utenti e profili a una configurazione mobile:

1. Dal menu a discesa Cerca, selezionare il tipo di membro da aggiungere: utenti o profili. Questo elenco a discesa non è disponibile se non è stata attivata la casella di controllo `Utente mobile` su qualunque record utente o se tutti gli utenti sono già assegnati a una configurazione mobile; in tal caso, è possibile assegnare profili solo a questa configurazione mobile.
2. Se il membro che si desidera aggiungere non è immediatamente visibile, immettere alcune parole chiave nella casella di ricerca e fare clic su **Trova**.
3. Selezionare gli utenti e i profili dalla casella `Membri disponibili`, quindi fare clic sulla freccia **Aggiungi** per aggiungerli alla configurazione mobile.

   È possibile assegnare ogni utente e profilo a una sola configurazione mobile.

   La casella `Membri disponibili` visualizza solo gli utenti per cui è stata attivata la casella di controllo `Utente mobile`.
4. Se nella casella `Membri assegnati` sono presenti utenti o profili che non si desidera assegnare a questa configurazione mobile, selezionarli e fare clic sulla freccia **Rimuovi**.

   Avvertenza: se si rimuove un utente da una configurazione mobile attiva, sul dispositivo mobile dell'utente vengono eliminati i dati relativi a Salesforce ma non l'applicazione client.

## Impostazione del limite alle dimensioni totali dei dati

I vari tipi di dispositivi mobili offrono diverse capacità di memoria, e per alcuni dispositivi di verificano seri problemi se viene utilizzata tutta la memoria flash. Per evitare di sovraccaricare i dispositivi mobili, è possibile specificare un limite alle dimensioni totali dei dati per ogni configurazione mobile. Il limite alle dimensioni totali dei dati impedisce che Salesforce invii una quantità eccessiva di dati ai dispositivi mobili degli utenti assegnati alla configurazione mobile.

Per impostare il limite alle dimensioni totali dei dati, utilizzare l'elenco a discesa `Non sincronizzare se le dimensioni dei dati superano:` per specificare la quantità di memoria che è normalmente disponibile sui dispositivi mobili degli utenti assegnati a questa configurazione mobile. Se le dimensioni combinate di tutte le serie di dati superano tale limite, gli utenti assegnati al profilo ricevono un messaggio di errore sui dispositivi mobili, e Salesforce non effettua la sincronizzazione delle serie di dati presenti in questa configurazione mobile. Verificare la configurazione mobile per accertarsi che le serie di dati non superino il limite alle dimensioni totali dei dati.

Suggerimento: per ridurre le dimensioni dei dati, eseguire una o più delle seguenti operazioni:

- Eliminare una serie di dati.
- Ridurre l'ambito delle serie di dati.
- Perfezionare i criteri di filtro delle serie di dati.

### Completamento della configurazione mobile

Fare clic su **Salva**. Tenere presente che la configurazione mobile non è attiva finché non si seleziona la casella di controllo `Attivo`.

VEDERE ANCHE:

Gestione delle configurazioni di Salesforce Classic mobile
Definizione di serie di dati
Impostazione di Salesforce Classic mobile

## Definizione di serie di dati

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le serie di dati mobili:
- "Visualizza impostazione e configurazione"

Per creare, modificare o eliminare le serie di dati mobili:
- "Gestisci configurazioni mobili"

L'accesso a Salesforce da un dispositivo mobile è molto diverso dall'accesso da un computer. Infatti, di solito i dispositivi mobili hanno meno memoria e uno schermo di dimensioni inferiori rispetto ai computer e non mantengono una connessione di rete costante. Per superare queste limitazioni, ogni configurazione mobile trasferisce solo serie di dati, cioè sottoinsiemi dei record a cui accedono gli utenti nell'interfaccia utente online di Salesforce. I dispositivi mobili memorizzano le serie di dati all'interno di database incorporati, per consentire agli utenti di accedere ai record più importanti e lavorare in modalità offline quando non è disponibile una connessione di rete. Salesforce sincronizza automaticamente i database incorporati quando il dispositivo mobile ristabilisce una connessione di rete.

Ogni serie di dati può contenere record relativi a un singolo oggetto e viene classificata in base al nome di tale oggetto. Ad esempio, la serie di dati Account include solo record di account.

Le serie di dati possono disporre di serie di dati secondarie, cioè di serie di dati che contengono i record associati alla serie di dati di livello massimo (superiore). Ad esempio, se il primo livello della gerarchia contiene una serie di dati Account, è possibile aggiungere una serie di dati secondaria Referenti che include tutti i record dei referenti correlati ai record degli account. Le serie di dati secondarie vengono visualizzate sui dispositivi mobili sotto forma di elenchi correlati.

Una singola configurazione mobile può contenere più serie di dati per lo stesso oggetto e a livelli diversi. Ad esempio, è possibile che sia presente una serie di dati principale Eventi e una serie di dati secondaria Eventi in Lead.

Dopo avere creato una configurazione mobile è necessario definirne le serie di dati. Per accedere alle serie di dati per una configurazione mobile:

1. Da Imposta, immettere *`Configurazioni Salesforce Classic`* nella casella `Ricerca veloce`, quindi selezionare **Configurazioni Salesforce Classic**. Fare clic sul nome della configurazione mobile che si desidera modificare.
2. Nell'elenco correlato Serie di dati, fare clic su **Modifica**.
3. Dalla pagina Serie di dati è possibile:
   - Aggiungere una serie di dati.
   - Per rimuovere una serie di dati, selezionarla e fare clic su **Rimuovi**.

- Per modificare una serie di dati, selezionarla nella gerarchia. Il riquadro destro visualizza i filtri per la serie di dati.
- Verificare la configurazione mobile.

Mentre si definiscono e modificano le serie di dati, Salesforce salva automaticamente le modifiche che vengono apportate.

4. Al termine, fare clic su **Chiudi**.

## Aggiunta di serie di dati

Per aggiungere una serie di dati:

1. Nella gerarchia, selezionare **Serie di dati** per creare una serie di dati principale oppure selezionare una serie di dati esistente per creare una serie di dati secondaria.
2. Fare clic su **Aggiungi...**
3. Nella finestra popup visualizzata, selezionare l'oggetto per i record che si desidera vengano inclusi nella serie di dati. Salesforce consente di creare serie di dati principali per tutti gli oggetti personalizzati e gli oggetti standard seguenti:
   - Account
   - Asset
   - Allegati
   - Casi
   - Referenti
   - Contenuto
   - Eventi
   - Lead
   - Note
   - Opportunità
   - Listini prezzi
   - Prodotti
   - Soluzioni
   - Operazioni
   - Utenti

   Nota:
   - Sebbene siano disponibili come serie di dati, gli allegati sono supportati solo in Salesforce Classic mobile per Android. Salesforce Classic mobile per iPhone e per BlackBerry attualmente non supportano gli allegati.
   - Salesforce Classic mobile supporta i valori predefiniti dei campi solo per gli elenchi di selezione e gli elenchi di selezione a selezione multipla. I valori predefiniti dei campi per altri tipi di campi, quali caselle di controllo e campi numerici, non sono visualizzati in Salesforce Classic mobile.

   Durante l'aggiunta a una serie di dati esistente, la finestra popup visualizza tutti gli oggetti che hanno una relazione con l'oggetto selezionato. Questi includono gli oggetti secondari e gli oggetti principali che hanno una relazione record principale-record dettaglio o una relazione di ricerca con l'oggetto selezionato.

   Ad esempio, si supponga di avere creato un campo account denominato Referente principale che ha una relazione di ricerca con l'oggetto referente. Se si aggiunge Account come serie di dati di livello massimo in una configurazione mobile, quando si aggiunge Referente sotto Account saranno visibili due serie di referenti:

   - **Referente:** rappresenta la relazione standard tra gli oggetti account e referente.

- **Referente (con riferimento da Account):** rappresenta qualsiasi oggetto che è il lato principale di una relazione di ricerca o di una relazione record principale-record dettaglio per l'oggetto selezionato. In questo caso, all'oggetto referente viene fatto riferimento mediante il campo Referente principale dell'oggetto account.

Poiché Salesforce fa distinzione tra questi due tipi di relazione, è possibile, ad esempio, rendere mobili solo i referenti cui si fa riferimento in un campo account personalizzato senza inviare al dispositivo alcun record di referente secondario.

4. Fare clic su **OK**. La serie di dati creata viene visualizzata nella gerarchia.
5. Se lo si desidera è possibile utilizzare i filtri per limitare i record inclusi in una serie di dati principale o secondaria:
   a. Utilizzare le opzioni Filtra per proprietà record per configurare Salesforce in modo che sincronizzi automaticamente i record in base al titolare. Le opzioni possibili sono:
      - `Tutti i record`: Salesforce sincronizza automaticamente tutti i record a cui può accedere l'utente. L'opzione `Tutti i record` non è disponibile per le operazioni e gli eventi quando questi sono serie di dati principali in una configurazione mobile. Questo consente di evitare la non riuscita di una sincronizzazione dati quando l'esecuzione delle query dei filtri di attività impiega troppo tempo.
      - `Record utente`: Salesforce sincronizza automaticamente tutti i record di proprietà dell'utente.
      - `Record del team utente`: Salesforce sincronizza automaticamente tutti i record di proprietà dell'utente e dei subordinati dell'utente nella gerarchia dei ruoli.
      - `Record del team account utente`: Salesforce sincronizza automaticamente gli account per i quali l'utente è membro del team account, ma non include gli account di cui l'utente è titolare.
      - `Record dei team opportunità utente`: Salesforce sincronizza automaticamente le opportunità per cui l'utente è membro del team opportunità, ma non include le opportunità di cui l'utente è titolare.
      - `Nessuno (Solo ricerca)`: Salesforce non sincronizza automaticamente alcun record della serie di dati; tuttavia, gli utenti possono utilizzare i dispositivi mobili per cercare tutti i record a cui possono accedere.

      Salesforce visualizza solo le opzioni correlate alla serie di dati selezionata. Ad esempio, se si seleziona una serie di dati account viene visualizzata l'opzione `Record dei team account utente`, mentre se si seleziona una serie di dati opportunità viene visualizzata l'opzione `Record dei team opportunità utente`.

      Se le esigenze di mobilità di un oggetto richiedono una combinazione dei filtri di proprietà dei record disponibili, è possibile aggiungere la stessa di serie di dati dell'oggetto fino a quattro volte sullo stesso livello di gerarchia. Ad esempio, un responsabile vendite può voler sincronizzare le sue opportunità, le opportunità di cui sono titolari i suoi sottoposti e le opportunità per le quali è un membro del team opportunità. In tal caso, aggiungere una serie di dati dell'opportunità e selezionare `Record del team utente`, quindi aggiungere una seconda serie di dati dell'opportunità allo stesso livello della gerarchia e selezionare `Record dei team opportunità utente`. Tenere presente che gli oggetti con una sola opzione di filtro proprietà, ad esempio Commento caso, non possono essere aggiunti più volte allo stesso livello della gerarchia.
   b. Impostare i criteri di filtro per sincronizzare automaticamente solo i record che soddisfano dei criteri specifici, oltre all'opzione Filtra per proprietà record selezionata. Ad esempio, è possibile impostare il filtro in modo che includa solo i record opportunità con un ammontare superiore a 50.000 € oppure i record dei referenti con il titolo “Addetto agli acquisti”.
   c. Per evitare che una singola serie di dati occupi tutta la memoria di un dispositivo mobile, selezionare il secondo pulsante di opzione sotto Imposta limite massimo dei record e immettere il numero massimo di record che la serie di dati può trasferire ai dispositivi mobili. Utilizzare gli elenchi a discesa Ordina per e Ordina per specificare quali record vengono sincronizzati se viene superato il limite alle dimensioni dei dati.

      Se viene raggiunto il limite, Salesforce aggiorna i record presenti sul dispositivo mobile ogni 20 minuti circa e sostituisce i record ogni 24 ore circa in base alle impostazioni di Ordina per e Ordina. Ad esempio, se le impostazioni sono Data ultima modifica e Discendente, Salesforce trasferisce i record modificati più di recente ai dispositivi mobili e rimuove lo stesso numero di record che sono stati modificati meno recentemente.

se è stata selezionata l'opzione `Nessuno (Solo ricerca)` per Filtra per proprietà record, il limite impostato non vale, perché nessun record viene sincronizzato automaticamente.

Suggerimento: non utilizzare l'opzione Imposta limite massimo dei record al posto dei filtri. Utilizzarla solo come meccanismo di sicurezza, e utilizzare i filtri come metodo principale di limitazione del numero di record presenti su un dispositivo mobile. In questo modo si garantisce che gli utenti mobili ricevano i record corretti sui dispositivi mobili.

A causa delle limitazioni di memoria nei dispositivi mobili, Salesforce impedisce che una sola query restituisca più di 2.500 record.

6. Ricordare di verificare la configurazione mobile per accertarsi che i dati non superino il limite alle dimensioni totali dei dati.
7. Fare clic su **Chiudi**.

VEDERE ANCHE:

Panoramica su Salesforce Classic mobile per gli amministratori

Gestione delle configurazioni di Salesforce Classic mobile

Impostazione di Salesforce Classic mobile

## Campi di unione per i criteri dei filtri mobili

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

Alcuni dei campi unione $User sono disponibili solo durante la definizione di filtri per le configurazioni mobili e le visualizzazioni personalizzate mobili. Nelle configurazioni mobili questi campi unione possono essere utilizzati per sincronizzare i record nei casi in cui un utente sia collegato a un record senza esserne il titolare. Ad esempio, è possibile inviare casi creati dall'utente attuale al dispositivo mobile o inviare record al dispositivo in cui si fa riferimento all'utente attuale in un campo personalizzato. Nelle visualizzazioni mobili è possibile utilizzare i campi unione per definire visualizzazioni in base al titolare dei record. Ad esempio è possibile creare una visualizzazione che mostri gli account correnti dell'utente con classificazione “Recente”.

La tabella seguente descrive i campi unione utente disponibili:

| Campo unione | Descrizione |
|---|---|
| `$User.ID` | Fa riferimento all'ID dell'utente attuale. Questo campo unione può essere applicato ai campi che contengono una ricerca utenti. Gli operatori validi per questo campo unione sono Uguale a e Non uguale a. Durante la creazione di filtri per visualizzazioni mobili che facciano riferimento a un campo titolare, è possibile utilizzare solo il campo unione `$User.ID`. |
| `$User.Username` | Fa riferimento al nome utente dell'utente attuale. Questo campo unione può essere applicato a qualsiasi campo di testo o di ricerca, ad eccezione degli elenchi di selezione. Gli operatori validi per questo campo unione sono Uguale a, Non uguale a, Maggiore o uguale a, Minore o uguale a, Contiene, Non contiene e Inizia con. |

| Campo unione | Descrizione |
| --- | --- |
| `$User.Firstname` | Fa riferimento al nome dell'utente attuale. Questo campo unione può essere applicato a qualsiasi campo di testo o di ricerca, ad eccezione degli elenchi di selezione. Gli operatori validi per questo campo unione sono Uguale a, Non uguale a, Maggiore o uguale a, Minore o uguale a, Contiene, Non contiene e Inizia con. |
| `$User.Lastname` | Fa riferimento al cognome dell'utente attuale. Questo campo unione può essere applicato a qualsiasi campo di testo o di ricerca, ad eccezione degli elenchi di selezione. Gli operatori validi per questo campo unione sono Uguale a, Non uguale a, Maggiore o uguale a, Minore o uguale a, Contiene, Non contiene e Inizia con. |
| `$User.Fullname` | Fa riferimento al nome e al cognome dell'utente attuale. Questo campo unione può essere applicato a qualsiasi campo di testo o di ricerca, ad eccezione degli elenchi di selezione. Gli operatori validi per questo campo unione sono Uguale a, Non uguale a, Maggiore o uguale a, Minore o uguale a, Contiene, Non contiene e Inizia con. |

VEDERE ANCHE:

Gestione delle configurazioni di Salesforce Classic mobile

Panoramica su Salesforce Classic mobile per gli amministratori

Definizione di serie di dati

## Verifica delle configurazioni di Salesforce Classic mobile

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le serie di dati di Salesforce Classic mobile:
- "Visualizza impostazione e configurazione"

Per verificare le configurazioni di Salesforce Classic mobile:
- "Gestisci configurazioni mobili"

Quando si crea una configurazione Salesforce Classic mobile, si definisce un limite alle dimensioni totali dei dati per la configurazione. Il limite alle dimensioni totali dei dati impedisce che Salesforce invii una quantità eccessiva di dati ai dispositivi mobili degli utenti assegnati alla configurazione mobile. Una volta definite le serie di dati, è importante verificare la configurazione mobile per assicurarsi che il limite alle dimensioni totali dei dati non venga superato.

Per stimare le dimensioni della serie di dati che la configurazione mobile invierà a un dispositivo utente:

1. Da Imposta, digitare *Configurazioni Salesforce Classic* nella casella `Ricerca veloce`, quindi selezionare **Configurazioni Salesforce Classic**. A questo punto, fare clic sul nome della configurazione mobile che si desidera verificare.
2. Nell'elenco correlato Serie di dati, fare clic su **Modifica**.
3. Nella sezione Test della dimensione dei dati, fare clic sull'icona di ricerca accanto al campo `Seleziona un utente` per scegliere l'utente da sottoporre a verifica. Nonostante gli utenti debbano essere abilitati per le comunicazioni wireless per poter essere assegnati a configurazioni mobili, la dimensione dei dati di una configurazione mobile può essere verificata per qualsiasi account utente.

   L'impostazione predefinita del campo `Seleziona un utente` corrisponde al nome dell'utente connesso; tuttavia, è importante verificare la configurazione mobile con gli account di tutti gli utenti che verranno effettivamente assegnati alla configurazione, in particolare degli utenti titolari di un elevato numero di record.

4. Selezionare la casella di controllo **Includi metadati** per fare in modo che i metadati vengano inclusi nella stima. I metadati sono informazioni relative ai layout di pagina e agli schemi; la quantità di metadati inviati a un dispositivo può essere molto grande in funzione delle dimensioni dell'organizzazione e della complessità della sua struttura.

   Avvertenza: il calcolo della dimensione dei metadati in aggiunta a quello della dimensione dei dati da parte di Salesforce potrebbe richiedere diversi minuti. Anche se si sceglie di nascondere i metadati nei risultati del test, questi vengono comunque calcolati nelle dimensioni totali dei dati quando il dispositivo mobile viene sincronizzato con Salesforce.

5. Fare clic su **Stima dimensione dei dati**.

   Viene calcolata la dimensione di ciascuna serie di dati. I risultati vengono visualizzati nella struttura della gerarchia, vale a dire nel riquadro sinistro dell'area della serie di dati nella parte superiore della pagina. Altri risultati vengono visualizzati nella sezione Test della dimensione dei dati, situata sotto la gerarchia.

   - Nella struttura della gerarchia, accanto a ogni serie di dati vengono visualizzati due numeri. Il primo rappresenta il numero di record generati dalla serie di dati, mentre il secondo rappresenta la dimensione totale della serie di dati in byte o kilobyte. Tale suddivisione risulta utile per identificare quali serie di dati potrebbero richiedere un ulteriore filtraggio per ridurne le dimensioni.
   - La sezione Test della dimensione dei dati offre una stima dei dati che la configurazione mobile attuale fornirebbe al dispositivo utente selezionato, fra cui:
     - La dimensione e il numero di record nell'insieme di dati di ogni oggetto.
     - Le dimensioni e il numero totale di record, compresi i record dell'insieme di dati e i record contrassegnati. Un record contrassegnato non fa parte della configurazione mobile di un utente. Esistono due modi per consentire ai record contrassegnati di diventare parte dell'insieme di dati:

- L'utente scarica i record sul suo dispositivo tramite le ricerche online e i record vengono contrassegnati in modo che possano essere inviati al dispositivo dell'utente a ogni sincronizzazione del dispositivo con Salesforce.
- I record nell'insieme di dati dell'utente contengono campi di ricerca per i record che non soddisfano i criteri di filtro della configurazione mobile. Salesforce sincronizza i record a cui viene fatto riferimento nei campi di ricerca in modo che gli utenti non trovino link interrotti nell'applicazione mobile.

  Suggerimento: Per un conteggio preciso dei record contrassegnati, sincronizzare i dati nell'applicazione mobile prima di stimare la dimensione dei dati. Per sincronizzare i dati:

  - Nei dispositivi Android, toccare **Info applicazione** > **Sincronizza ora** > **Aggiorna tutti i dati**.
  - Nei dispositivi BlackBerry, visualizzare il menu e selezionare **System Info**, quindi visualizzare il menu e selezionare **Refresh All Data**.
  - Nei dispositivi iPhone, toccare **More**, quindi **App Info**. Selezionare **Sync Now**, quindi **Refresh All Data**.

- Le dimensioni dei metadati che verrebbero inviati al dispositivo dell'utente se si selezionasse la casella di controllo **Includi metadati**.
- L'insieme totale dei dati resi disponibili su dispositivo mobile, vale a dire la somma di tutti i record.

- I rapporti non sono inclusi nella stima delle dimensioni dei dati.

6. Confrontare i risultati della verifica con il limite alle dimensioni totali dei dati impostato per la configurazione; tale limite è visualizzato nella parte superiore della sezione Test della dimensione dei dati. Fare clic sul limite alle dimensioni dei dati per incrementare o ridurre tale valore nella pagina Modifica configurazione mobile.
   - Se la dimensione totale dei dati è inferiore al limite, l'utente selezionato può essere assegnato senza problemi alla configurazione mobile. Tuttavia, tenere presente che i risultati del test sono solo una stima, in quanto ogni dispositivo prevede algoritmi di archiviazione differenti.
   - Se la dimensione totale dei dati supera il limite, ridurla mediante riduzione dell'ambito della serie di dati, perfezionamento dei criteri di filtro delle serie di dati, eliminazione di una serie di dati o rimozione di campi dal layout di pagina mobile. Ripetere la procedura di verifica fino a quando la dimensione dei dati non rientra nel limite totale.

     Nota: la stima della dimensione totale dei dati nella sezione Test della dimensione dei dati non viene aggiornata automaticamente quando si modificano le serie di dati. Per aggiornare i risultati, fare clic su **Aggiorna dimensione dei dati**.

VEDERE ANCHE:

Panoramica su Salesforce Classic mobile per gli amministratori
Gestione delle configurazioni di Salesforce Classic mobile
Gestione dei dispositivi di Salesforce Classic mobile
Impostazione di Salesforce Classic mobile

## Modifica delle proprietà degli oggetti per Salesforce Classic mobile

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le configurazioni di Salesforce Classic mobile:
- "Visualizza impostazione e configurazione"

Per modificare le proprietà degli oggetti di Salesforce Classic mobile:
- "Gestisci configurazioni mobili"

È possibile modificare le proprietà degli oggetti standard e personalizzati nell'applicazione Salesforce Classic mobile. Ad esempio, si possono limitare le autorizzazioni degli utenti di Salesforce Classic mobile oppure escludere campi non necessari dal layout di pagina mobile dell'oggetto.

Le proprietà degli oggetti di Salesforce Classic mobile sono personalizzate in base alla configurazione mobile. Per modificare le proprietà degli oggetti mobili:

1. Da Imposta, digitare `Configurazioni Salesforce Classic` nella casella `Ricerca veloce`, quindi selezionare **Configurazioni Salesforce Classic**.
2. Fare clic sul nome della configurazione mobile che si desidera modificare.
3. Nell'elenco correlato Proprietà oggetto mobile, fare clic su **Modifica** accanto al nome di un oggetto.

   Nell'elenco correlato vengono visualizzati solo gli oggetti dell'insieme di dati di configurazione che sono stati resi disponibili su dispositivi mobili. Non è possibile modificare le proprietà dell'oggetto utente.

4. Dalla pagina Modifica configurazione mobile, è possibile:
   - Eliminare autorizzazioni per oggetti mobili
   - Personalizzare i layout di pagina di Salesforce Classic mobile
5. Fare clic su **Salva**.

### Eliminare autorizzazioni per oggetti mobili

L'applicazione Salesforce Classic mobile eredita le autorizzazioni degli utenti da Salesforce. Alcuni amministratori preferiscono limitare ulteriormente le autorizzazioni degli utenti che accedono ai dati Salesforce nell'applicazione Salesforce Classic mobile, solitamente a causa delle limitazioni dell'applicazione o della possibilità di un errore da parte degli utenti. Gli utenti possono ad esempio cancellare involontariamente un record senza rendersi conto che eliminando un record in Salesforce Classic mobile lo si elimina anche in Salesforce. Se questo pericolo è reale, gli amministratori possono impedire agli utenti di eliminare record dall'applicazione mobile, indipendentemente dalle autorizzazioni relative a oggetti standard e personalizzati di cui possano godere in Salesforce. Inoltre, Salesforce Classic mobile non supporta tutte le funzionalità di Salesforce, come S-Control e Apex. Se il processo aziendale relativo a un oggetto non è supportato da Salesforce Classic mobile, è possibile impedire agli utenti mobili di aggiornare tali record nell'applicazione.

Nella sezione Autorizzazioni, selezionare le autorizzazioni per gli utenti mobili da eliminare per l'oggetto. Utilizzare le caselle di controllo **Nega creazione**, **Nega modifica** o **Nega eliminazione** per impedire agli utenti di creare, modificare o eliminare record in Salesforce Classic mobile.

Nota: attualmente non è possibile bloccare le autorizzazioni mobili per l'oggetto contenuto.

### Personalizzare i layout di pagina di Salesforce Classic mobile

L'applicazione Salesforce Classic mobile eredita i layout di pagina degli utenti da Salesforce. È possibile che gli amministratori desiderino escludere alcuni campi dal layout di pagina mobile di ciascun oggetto, in quanto i campi non necessari possono occupare memoria e rendere meno fluido lo scorrimento delle pagine sul dispositivo mobile.

Nella sezione Campi esclusi selezionare i campi da visualizzare sul dispositivo mobile per l'oggetto selezionato. Per aggiungere o rimuovere i campi, selezionare il nome di un campo e fare clic sulla freccia **Aggiungi** o **Rimuovi**.

- Gli amministratori possono visualizzare tutti i campi disponibili per oggetto, indipendentemente dalla protezione a livello di campo.
- Alcuni campi sono obbligatori perché consentono a Salesforce Classic mobile di comunicare con Salesforce. Tali campi non vengono visualizzati nella casella Campi disponibili perché sono obbligatori e non possono essere pertanto esclusi dai layout di pagina mobili.
- I campi utilizzati nelle visualizzazioni personalizzate mobili non si possono escludere dai layout di pagina mobili.
- Se l'oggetto contenuto viene reso disponibile sui dispositivi mobili, tutti i campi dell'oggetto contenuto sono visualizzati nella casella Campi disponibili; tuttavia, il layout della pagina dei dettagli del contenuto nell'applicazione Salesforce Classic mobile è codificato nel programma in modo da visualizzare solo determinati campi. L'esclusione di campi dell'oggetto contenuto non influisce sul layout di pagina nell'applicazione.

VEDERE ANCHE:

Panoramica su Salesforce Classic mobile per gli amministratori

Gestione delle configurazioni di Salesforce Classic mobile

Gestione delle schede di Salesforce Classic mobile

Creazione di link al Web e alle pagine Visualforce Mobile per Salesforce Classic mobile

Impostazione di Salesforce Classic mobile

## Assegnazione di schede a una configurazione Salesforce Classic mobile

Per ciascuna configurazione mobile è possibile selezionare le schede che compaiono nell'applicazione Salesforce Classic mobile e definirne l'ordine. Le schede disponibili per una configurazione mobile comprendono:

- Schede Oggetto standard
- Schede Oggetto personalizzato
- Schede Visualforce e Web che sono state abilitate per Salesforce Classic mobile

> Avvertenza: non tutti i siti Web e le funzionalità di Visualforce sono supportati dai dispositivi mobili. Leggere con attenzione le procedure consigliate per creare pagine idonee per i dispositivi mobili prima di abilitare le schede Visualforce o Web per l'applicazione Salesforce Classic mobile.

Per impostazione predefinita, le schede funzionano allo stesso modo nell'applicazione Salesforce Classic mobile e nel sito Salesforce completo: se la scheda di un oggetto è nascosta in Salesforce, è nascosta anche in Salesforce Classic mobile.

> Nota: Se si personalizzano le schede mobili, le schede selezionate per la configurazione mobile vengono inviate ai dispositivi mobili degli utenti anche se le schede non sono state aggiunte a una configurazione. Le schede inviate al dispositivo vengono visualizzate nell'applicazione Salesforce Classic mobile solo se gli utenti dispongono dell'autorizzazione per visualizzarle.

Esistono diversi motivi per nascondere la scheda di un oggetto in Salesforce Classic mobile anche se i record dell'oggetto vengono inviati al dispositivo. L'app Salesforce Classic mobile dispone di molto meno spazio sullo schermo per visualizzare una riga di schede, così in alcuni casi è possibile scegliere di ridurre il numero di schede sul dispositivo. A volte inoltre un oggetto personalizzato dispone di una relazione con un oggetto standard, e gli utenti accedono al record dell'oggetto personalizzato attraverso il record dell'oggetto principale. In questo caso è possibile rendere mobile l'oggetto personalizzato ma nasconderne la scheda.

Per assegnare le schede a una configurazione mobile:

1. Da Imposta, immettere `Configurazioni Salesforce Classic` nella casella `Ricerca veloce`, quindi selezionare **Configurazioni Salesforce Classic**. Fare clic sul nome di una configurazione mobile.
2. Nell'elenco correlato Schede mobili, fare clic su **Personalizza schede** per definire le schede mobili per la prima volta. Se le schede mobili sono già state impostate, fare clic su **Modifica**.
3. Selezionare le schede dall'elenco `Schede disponibili`, quindi fare clic sulla freccia **Aggiungi** per aggiungerle alla configurazione mobile.
4. Nell'elenco `Schede selezionate` scegliere le schede e fare clic sulle frecce **Su** e **Giù** per disporre le schede nell'ordine in cui devono apparire nell'app Salesforce Classic mobile.
5. Fare clic su **Salva**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le configurazioni di Salesforce Classic mobile:

- "Visualizza impostazione e configurazione"

Per personalizzare le schede di Salesforce Classic mobile:

- "Gestisci configurazioni mobili"

Nota: gli utenti iPhone possono personalizzare l'ordine delle schede nell'app Salesforce Classic mobile. Se l'utente personalizza l'ordine delle schede, le eventuali modifiche apportate dall'amministratore nella configurazione mobile vengono ignorate dall'app e le nuove schede rese disponibili su dispositivo mobile vengono aggiunte al di sotto di quelle esistenti dell'utente.

VEDERE ANCHE:

Gestione delle schede di Salesforce Classic mobile
Abilitazione delle schede Web e Visualforce per Salesforce Classic mobile
Panoramica su Salesforce Classic mobile per gli amministratori
Gestione delle configurazioni di Salesforce Classic mobile

## Abilitazione delle schede Web e Visualforce per Salesforce Classic mobile

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

È possibile rendere disponibili le schede Web e Visualforce nell'app Salesforce Classic mobile. Quando si crea la scheda Web o la scheda Visualforce, modificare le proprietà delle schede e selezionare la casella di controllo `Pronto per Salesforce Classic mobile` per verificare che la pagina Web o la pagina Visualforce sia visualizzata e funzioni correttamente su un dispositivo mobile. Selezionando la casella di controllo si aggiunge la scheda all'elenco delle schede disponibili per le configurazioni Salesforce Classic mobile mobili.

È importante notare che la maggior parte dei browser mobili presenta limitazioni tecniche in termini di dimensioni della visualizzazione, script, velocità del processore e latenza di rete. Verificare le seguenti considerazioni prima di rendere mobili le proprie pagine Web e Visualforce per accertarsi che siano compatibili con i browser mobili.

### Considerazioni sulle schede Web mobili

Durante la definizione di una scheda Web che verrà utilizzata nell'app Salesforce Classic mobile prestare attenzione ai seguenti punti:

- La possibilità di rendere mobili le schede Web è disponibile solo per i dispositivi BlackBerry e iPhone. Se si rende mobile una scheda Web, tenere presente che gli utenti Android non saranno in grado di visualizzare la scheda in Salesforce Classic mobile.
- Le schede Web necessitano almeno del sistema operativo BlackBerry versione 4.3.
- Il tipo di scheda deve essere URL. L'applicazione mobile non può eseguire S-Control.
- Alcune pagine Web contengono JavaScript e Flash, ma non tutti i browser mobili li supportano:
  - Il browser Safari di Apple supporta JavaScript, ma non Flash.
  - Il browser BlackBerry ha un supporto limitato per JavaScript e nessun supporto per Flash.
- Prima di rendere mobile una scheda Web, passare all'URL di destinazione su uno dei dispositivi mobili della propria organizzazione per verificare se funziona come previsto in un browser mobile. Nel caso in cui la dotazione di dispositivi dell'organizzazione comprenda telefoni con sistemi operativi diversi (ad esempio sia smartphone iPhone che BlackBerry) effettuare il test su ogni tipo di apparecchio. Se gli utenti non riescono ad eseguire le operazioni necessarie nella pagina Web da un browser mobile, non rendere mobile la scheda Web.
- Per poter visualizzare le pagine Web JavaScript, JavaScript deve essere abilitato sui dispositivi BlackBerry. L'amministratore BlackBerry può abilitare globalmente JavaScript dal server Enterprise di BlackBerry. Gli utenti possono inoltre abilitare JavaScript su uno smartphone BlackBerry aprendo il browser BlackBerry, selezionando **Opzioni** > **Configurazione browser**, quindi selezionando la casella di controllo **Supporta JavaScript**.

### Considerazioni sulle schede mobili Visualforce

Considerare quanto segue per definire una scheda Visualforce mobile:

- Visualforce Mobile è disponibile solo per BlackBerry e iPhone. Se si rende mobile una scheda Visualforce, tenere presente che gli utenti Android non saranno in grado di visualizzare la scheda in Salesforce Classic mobile.
- L'app Salesforce Classic mobile può essere eseguita sul sistema operativo BlackBerry dalla versione 4.3 alla versione 7.0. Per ottenere prestazioni ottimali, tuttavia, Salesforce consiglia di installare almeno la versione 6.0 di Visualforce Mobile sugli smartphone BlackBerry.
- Poiché le dimensioni di visualizzazione sono limitate nei browser mobili, è consigliabile riorganizzare la pagina Visualforce in modo da ottimizzarla per gli utenti mobili:
  - Impostare gli attributi `sidebar` e `showHeader` nel tag `<apex:page>` su `false`. I telefoni sono caratterizzati da schermi di dimensioni ridotte e da una potenza di elaborazione limitata: è quindi indispensabile che l'intestazione laterale e l'intestazione della scheda vengano rimosse dalla pagina.
  - Impostare l'attributo `standardStylesheets` nel tag `<apex:page>` su `false`. Con il foglio di stile Salesforce standard, le pagine vengono caricate lentamente nel dispositivo. Inoltre, la maggior parte dei browser BlackBerry con sistema operativo precedente alla versione a 6.0 non sono in grado di interpretare correttamente i fogli di stile CSS. La soluzione migliore per aggiungere un foglio di stile alla pagina è aggiungere una sezione `<style>` subito al di sotto del componente `<apex:page>`.
  - Impostare l'attributo `columns` nel componente `<apex:pageBlockSection>` su `1`. Sullo schermo di un dispositivo mobile non c'è abbastanza spazio per visualizzare due colonne. Specificando un layout a una sola colonna, si evita quindi una disposizione scorretta dei campi.
- Le pagine di avvio non vengono visualizzate nell'app Salesforce Classic mobile.
- Nell'app Salesforce Classic mobile, la pagina Visualforce viene incorporata in una scheda, quindi è opportuno evitare l'uso delle schede per la navigazione nelle pagine Visualforce mobili.
- Anche se l'utente sa che il browser mobile supporta il codice JavaScript nella pagina Visualforce, dovrà ridurre al minimo l'uso di tale codice. I dispositivi mobili generalmente hanno connessioni di rete lente e troppi script in esecuzione in una pagina creano problemi di prestazioni. Per ridurre al minimo la quantità di codice JavaScript nelle pagine Visualforce mobili, provare a creare le pagine utilizzando prevalentemente HTML.
- Tutte le pagine Visualforce contengono JavaScript, anche se non si creano pagine che utilizzano il codice JavaScript. Per poter visualizzare le pagine Visualforce, JavaScript deve essere abilitato sui dispositivi BlackBerry. L'amministratore BlackBerry può abilitare globalmente JavaScript dal server Enterprise di BlackBerry. Gli utenti possono inoltre abilitare JavaScript su uno smartphone BlackBerry aprendo il browser BlackBerry, selezionando **Opzioni** > **Configurazione browser**, quindi selezionando la casella di controllo **Supporta JavaScript**.
- Il browser integrato nell'applicazione client del BlackBerry non dispone della funzione di navigazione incorporata. Se la pagina Visualforce è una procedura guidata è necessario predisporre dei link per la navigazione che consentano di tornare alla pagina precedente e di procedere a quella successiva.
- Gli amministratori BlackBerry devono tenere presente che l'impostazione delle dimensioni di download in BlackBerry Enterprise Server influisce sulla quantità di dati che verrà trasferita sul dispositivo. Verificare che tale impostazione sia adeguata ed effettuare un test delle pagine Visualforce prima di distribuirle agli utenti Salesforce Classic mobile.
- È possibile eseguire un'analisi dell'agente utente in un controller personalizzato per supportare più dispositivi. L'operazione può essere eseguita analizzando il risultato appropriato del metodo `getHeaders()` nel riferimento alla pagina corrente.

VEDERE ANCHE:

Gestione delle schede di Salesforce Classic mobile

Gestione delle configurazioni di Salesforce Classic mobile

Creazione di link al Web e alle pagine Visualforce Mobile per Salesforce Classic mobile

Assegnazione di schede a una configurazione Salesforce Classic mobile

## Creazione di visualizzazioni elenco per Salesforce Classic mobile

È possibile creare visualizzazioni elenco personalizzate per gli utenti Salesforce Classic mobile. Le visualizzazioni elenco personalizzate per Salesforce Classic mobile, dette anche visualizzazioni mobili, si differenziano dalle visualizzazioni personalizzate di Salesforce per i seguenti aspetti:

- Gli amministratori impostano le visualizzazioni mobili per ciascuna configurazione mobile. Le visualizzazioni sono disponibili a tutti gli utenti assegnati alla configurazione e gli amministratori non possono limitare la visibilità a determinati gruppi di utenti all'interno della configurazione. Ogni oggetto reso disponibile su dispositivo mobile in una configurazione mobile può avere un massimo di 10 visualizzazioni personalizzate.
- Gli utenti non possono filtrare le visualizzazioni mobili in base a Tutti i record o Record personali. Le visualizzazioni sono applicabili a tutti i record archiviati localmente sul dispositivo a prescindere dal titolare; tuttavia, è possibile applicare dei filtri di proprietà utilizzando i campi addizionali nei criteri di ricerca.
- Le visualizzazioni mobili non supportano la logica dei filtri.
- Le visualizzazioni mobili sono limitate a una visualizzazione a due colonne.
- Gli utenti possono ordinare le visualizzazioni mobili in modo crescente o decrescente in base a un massimo di due campi.

Per ogni configurazione mobile, è possibile definire un massimo di 10 visualizzazioni personalizzate per ogni oggetto. Queste visualizzazioni vengono in seguito inviate ai dispositivi degli utenti assegnati alle configurazioni interessate. Per creare una visualizzazione personalizzata per Salesforce Classic mobile:

1. Da Imposta, immettere *Configurazioni Salesforce Classic* nella casella `Ricerca veloce`, quindi selezionare **Configurazioni Salesforce Classic**. Fare clic sul nome di una configurazione mobile. Potrebbe essere necessario creare una configurazione mobile se non è già stato fatto.
2. Scorrere fino all'elenco correlato Visualizzazioni mobili
3. Scegliere un tipo di oggetto dall'elenco a discesa Selezionare un oggetto e fare clic su **Nuova visualizzazione mobile**. Nell'elenco a discesa vengono visualizzati solo gli oggetti inclusi nella serie di dati della configurazione mobile. Non è possibile creare visualizzazioni mobili per l'oggetto utente.
4. Immettere il nome della visualizzazione.

   Poiché lo spazio di visualizzazione sui dispositivi mobili è limitato, la lunghezza massima di un nome per una visualizzazione mobile è di 30 caratteri.

5. Nella sezione Specifica i criteri di filtro, immettere le condizioni che gli elementi selezionati devono soddisfare, ad esempio *Importo maggiore di 100000 $*.
   a. Scegliere un campo dal primo elenco a discesa.

      Nota: Non è consentito creare visualizzazioni in base ai campi esclusi dai layout di pagina mobile o ai campi che sono nascosti per tutti i profili e gli insiemi di autorizzazioni.

   b. Scegliere un operatore filtro.
   c. Nel terzo campo inserire il valore di cui individuare la corrispondenza.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare utenti e dispositivi di Salesforce Classic mobile:

- "Visualizza impostazione e configurazione"

Per gestire le visualizzazioni personalizzate di Salesforce Classic mobile:

- "Gestisci configurazioni mobili"

Avvertenza: tenere presente quanto segue in merito ai valori dei criteri per le visualizzazioni mobili:

- Per fare riferimento all'utente corrente, è possibile utilizzare il campo di unione `$User.ID` come valore nei criteri di filtro. Non è possibile immettere nomi utente nei criteri di filtro.
- Nei criteri di filtro è possibile immettere solo valori di data speciali, non le date effettive.
- Nei criteri di filtro non è possibile utilizzare valori di data speciali FISCALI.

d. Selezionare **Fai corrispondere tutto** se le voci nella visualizzazione mobile devono soddisfare tutti i criteri inseriti. Selezionare **Fai corrispondere uno qualsiasi** se le voci nella visualizzazione mobile devono soddisfare uno qualsiasi dei criteri inseriti. le visualizzazioni personalizzate mobili non supportano le opzioni di filtro avanzate.

6. Nella sezione Seleziona i campi da visualizzare, selezionare i campi da utilizzare come colonne di visualizzazione.

   I campi predefiniti vengono selezionati automaticamente. È possibile scegliere fino a due colonne diverse di campi di dati da visualizzare nella visualizzazione personalizzata mobile.

7. Nella sezione Definisci l'ordinamento, se lo si desidera è possibile impostare un ordinamento primario e secondario per la visualizzazione.

   a. Scegliere un campo dall'elenco a discesa Ordina per. È possibile ordinare in base ai campi che sono stati esclusi dal layout di pagina mobile dell'oggetto.

   b. Impostare l'ordine su Crescente o Decrescente.

8. Fare clic su **Salva**.

VEDERE ANCHE:

Gestione delle visualizzazioni di Salesforce Classic mobile
Gestione delle configurazioni di Salesforce Classic mobile
Gestione dei dispositivi di Salesforce Classic mobile
Impostazione di Salesforce Classic mobile

## Impostazione dell'applicazione Mobile Dashboards for iPad

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le configurazioni mobili:
- "Visualizza impostazione e configurazione"

Per rendere mobili i cruscotti digitali:
- "Gestisci configurazioni mobili"

Importante: A partire dal rilascio Summer '15, l'applicazione Mobile Dashboards for iPad non è più supportata. È possibile continuare a utilizzare l'applicazione, ma Salesforce non fornisce più l'assistenza sotto forma di correzioni di bug o ottimizzazioni per eventuali problemi che gli utenti dovessero riscontrare. Rivolgersi all'amministratore Salesforce per la migrazione all'app Salesforce1, la nuova esperienza mobile di Salesforce.

La scheda Cruscotti digitali può essere resa disponibile in Salesforce Classic mobile aggiungendola alle schede di una configurazione mobile. I cruscotti digitali mobili consentono agli utenti fuori sede di rimanere aggiornati sul contesto aziendale e sugli indicatori di prestazione anche quando non sono fisicamente in ufficio.

Tenere presente quanto segue riguardo ai cruscotti digitali mobili.

- La scheda Cruscotti digitali nell'applicazione mobile avvia un browser incorporato per la visualizzazione dei cruscotti digitali.
- A causa delle dimensioni dello schermo limitate, i cruscotti digitali mobili vengono visualizzati su un'unica colonna.
- Nei cruscotti digitali mobili, i link ai dettagli dei rapporti personalizzati sono disattivati.
- La prima volta che un utente visita la scheda Cruscotti digitali in Salesforce Classic mobile, l'applicazione mobile richiede l'ultimo cruscotto digitale visualizzato dall'utente in Salesforce. In base all'intensità del segnale WiFi o del cellulare, potrebbero essere necessari alcuni minuti prima che il cruscotto digitale venga visualizzato nella pagina.
- I cruscotti digitali non vengono aggiornati automaticamente nell'applicazione mobile. Gli utenti possono richiedere un aggiornamento del cruscotto digitale facendo clic sul pulsante **Aggiorna**.
- Nell'applicazione mobile, gli utenti possono lavorare in modalità offline. Senza una connessione wireless, gli utenti possono visualizzare l'ultimo cruscotto digitale visualizzato, ma non possono aggiornarlo o selezionarne un altro.
- Per i cruscotti digitali mobili, i dispositivi BlackBerry devono disporre almeno del sistema operativo versione 4.5. I cruscotti digitali mobili sono compatibili con la versione 4.3, ma le tabelle dei cruscotti digitali potrebbero non essere visualizzate correttamente.
- Gli amministratori dei dispositivi BlackBerry devono tenere presente che l'impostazione della quantità di dati scaricabili in BlackBerry Enterprise Server influisce sulla quantità di dati del cruscotto digitale che è possibile inviare al dispositivo. Verificare che l'impostazione della quantità di dati scaricabili sia corretta ed eseguire un test sui cruscotti digitali prima di distribuirli agli utenti mobili.

Nota: attualmente i cruscotti digitali sono disponibili sono nelle applicazioni client mobili BlackBerry e iPhone.

Per abilitare i cruscotti digitali mobili:

1. Da Imposta, immettere `Cruscotti digitali mobili` nella casella `Ricerca veloce`, quindi selezionare **Impostazioni cruscotti digitali mobili**. Fare clic sul nome di una configurazione mobile.
2. Nell'elenco correlato Schede mobili, fare clic su **Personalizza schede** per definire le schede mobili per la prima volta. Se le schede mobili sono già state impostate, fare clic su **Modifica**.
3. Selezionare **Cruscotti digitali** dall'elenco Schede disponibili, quindi fare clic sulla freccia **Aggiungi** per aggiungerla alla configurazione mobile. L'elenco Schede disponibili include le schede di oggetti standard e le schede di oggetti personalizzati. Può anche includere le schede Web e Visualforce.

   Avvertenza: se nella configurazione mobile non vi sono ancora schede personalizzate, è necessario selezionare tutte le schede che si desidera visualizzare nell'applicazione mobile e non solo la scheda Cruscotti digitali.

4. Nell'elenco Schede selezionate, scegliere la scheda Cruscotti digitali e fare clic sulle frecce **Su** e **Giù** per definire l'ordine in cui la scheda Cruscotti digitali deve apparire nell'applicazione mobile.

5. Fare clic su **Salva**.

VEDERE ANCHE:

Impostazione di Salesforce Classic mobile

## Abilitazione dei rapporti in Salesforce Classic mobile

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per creare, modificare ed eliminare cartelle di rapporti pubblici:
- "Gestisci rapporti pubblici"

Per visualizzare le configurazioni di Salesforce Classic mobile:
- "Visualizza impostazione e configurazione"

Per abilitare i rapporti nell'applicazione Salesforce Classic mobile:

1. Creare una cartella Rapporti mobili in Salesforce. Dalla pagina iniziale dei rapporti nel sito completo, fare clic su **Crea nuova cartella**.
2. Nel campo `Cartella rapporti`, immettere: *`Rapporti mobili`*.

   Il server non caricherà i rapporti sui dispositivi mobili finché alla cartella non viene assegnato il nome `Rapporti mobili`. Prima di salvare la cartella, assicurarsi che il suo nome non contenga refusi. Inoltre, Salesforce non richiede che i nomi delle cartelle siano univoci. Gli utenti di Salesforce Classic mobile possono visualizzare i rapporti archiviati in tutte le cartelle denominate Rapporti mobili a meno che non venga limitato l'accesso con l'opzione di visibilità della cartella.

3. Scegliere un'opzione di `Accesso a cartelle pubbliche`. Questa opzione non influisce sulla possibilità degli utenti mobili di eseguire i rapporti.
4. Se lo si desidera, selezionare un rapporto non archiviato e fare clic su **Aggiungi** per memorizzarlo nella cartella Rapporti mobili. È anche possibile aggiungere rapporti alla cartella dopo averla salvata.
5. Scegliere un'opzione di visibilità della cartella.
   - `Questa cartella è accessibile a tutti gli utenti` consente a tutti gli utenti dell'organizzazione di visualizzare l'elenco dei rapporti mobili dai loro dispositivi.
   - `Questa cartella è accessibile solo ai seguenti utenti` consente di concedere l'accesso solo a un gruppo di utenti selezionati.

     Non rendere privata la cartella `Rapporti mobili` a meno che l'utente non desideri nascondere i rapporti mobili a tutti gli utenti, incluso se stesso.

6. Fare clic su **Salva**.
7. Aggiungere i rapporti alla cartella Rapporti mobili. Fare clic sul nome del rapporto nella pagina iniziale dei rapporti, quindi fare clic su **Salva con nome** e salvare il rapporto nella cartella Rapporti mobili.

   Dopo aver salvato il rapporto, è possibile modificare le opzioni per facilitare la visualizzazione sui dispositivi mobili. Ad esempio, è possibile ridurre il numero di colonne o immettere criteri di filtro aggiuntivi.

8. Aggiungere la scheda Rapporti alle configurazioni mobili. Da Imposta, digitare *`Configurazioni Salesforce Classic`* nella casella `Ricerca veloce`, quindi selezionare **Configurazioni Salesforce Classic**. Fare clic sul nome di una configurazione mobile.
9. Nell'elenco correlato Schede mobili, fare clic su **Personalizza schede** per definire le schede mobili per la prima volta. Se le schede mobili sono già state impostate, fare clic su **Modifica**.

10. Selezionare **Rapporti** dall'elenco Schede disponibili, quindi fare clic sulla freccia **Aggiungi** per aggiungerla alla configurazione mobile. L'elenco Schede disponibili include le schede di oggetti standard e le schede di oggetti personalizzati. Può anche includere le schede Web e Visualforce.

    Avvertenza: Se nella configurazione mobile non vi sono ancora schede personalizzate, è necessario selezionare tutte le schede che si desidera visualizzare in Salesforce Classic mobile e non solo la scheda Rapporti.

11. Nell'elenco Schede selezionate, scegliere la scheda Rapporti e fare clic sulle frecce **Su** e **Giù** per definire il punto in cui deve apparire la scheda Rapporti nell'applicazione Salesforce Classic mobile.
12. Fare clic su **Salva**.

Nota: Attualmente, i rapporti di Salesforce Classic mobile non sono disponibili sui dispositivi Android o iPhone.

VEDERE ANCHE:

Impostazione di Salesforce Classic mobile

## Impostazione di Salesforce CRM Content per Salesforce Classic mobile

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le configurazioni di Salesforce Classic mobile:

- "Visualizza impostazione e configurazione"

Per creare, modificare o eliminare serie di dati di Salesforce Classic mobile:

- "Gestisci configurazioni mobili"

Tenere presente quanto segue relativamente alle modalità di implementazione di Salesforce CRM Content in Salesforce Classic mobile:

- Le informazioni del record contenuto vengono sincronizzate con il dispositivo, ma questo non avviene per i file associati ai record contenuto. Questo consente agli utenti di consegnare contenuti dall'applicazione anche quando un file è troppo grande per essere scaricato su un dispositivo mobile.
- Gli utenti non possono cercare un contenuto specifico nell'applicazione: possono solo condividere i contenuti disponibili nella scheda Contenuto, che viene sincronizzata automaticamente con il loro dispositivo secondo i filtri della configurazione mobile loro assegnata.
- Gli utenti non possono visualizzare un elenco dei contenuti a cui sono abbonati nell'applicazione. Non possono inoltre filtrare l'elenco dei record nella scheda Contenuto in base a una determinata libreria.
- Benché possano visualizzare in anteprima e condividere i contenuti dall'applicazione, gli utenti non possono aggiornare il file associato a un record contenuto. Se dispongono delle autorizzazioni necessarie, possono modificare i campi della pagina dei dettagli del contenuto.
- Gli utenti devono disporre di una connessione dati per visualizzare in anteprima e fornire i contenuti. Senza una connessione dati possono visualizzare solo la pagina dei dettagli del contenuto.
- In Salesforce Classic mobile, il contenuto è supportato solo sui dispositivi BlackBerry e iPhone.
- Il contenuto non è disponibile nella versione gratuita di Salesforce Classic mobile.
- Non è possibile bloccare le autorizzazioni mobili per l'oggetto contenuto. In Salesforce Classic mobile, l'oggetto contenuto è al momento di sola lettura.
- Non è possibile modificare il layout di pagina mobile per l'oggetto contenuto. La pagina dei dettagli del contenuto nell'applicazione è codificata per visualizzare solo alcuni campi.

Per impostare il contenuto per una configurazione Salesforce Classic mobile:

1. Da Imposta, digitare *Configurazioni Salesforce Classic* nella casella Ricerca veloce, quindi selezionare **Configurazioni Salesforce Classic** e fare clic sul nome di una configurazione mobile.
2. Nell'elenco correlato Serie di dati, fare clic su **Modifica**.
3. Fare clic su **Aggiungi...**
4. Nella finestra popup, selezionare Contenuto e fare clic su **OK**.
5. Specificare mediante i filtri campo i record contenuto da sincronizzare.

   Poiché gli utenti non possono cercare contenuti nell'applicazione Salesforce Classic mobile, è essenziale impostare dei filtri che rendano disponibili i contenuti importanti sul dispositivo. Tali filtri non si possono creare in base alle librerie o agli abbonamenti, ma di seguito sono descritte alcune possibilità per impostare delle condizioni di filtro utili:

   - **Date:** Filtro sui campi Data ultima modifica, Data modifica contenuto o Data creazione. Utilizzare valori di date speciali quali ULTIMI 90 GIORNI o ULTIMI 180 GIORNI per far sì che i record contenuto aggiornati di recente vengano sincronizzati.
   - **Titolare:** Applicare un filtro all'autore se all'interno dell'organizzazione la pubblicazione del contenuto è affidata a persone specifiche.
   - **Tipo di file:** Applicare un filtro su determinati tipi di documenti. Ad esempio, al team opportunità in genere interessano le presentazioni o i documenti in formato PDF.
   - **Campi personalizzati:** Se sono stati creati campi contenuto personalizzati per facilitare la classificazione dei contenuti, applicare un filtro sui campi personalizzati. Ad esempio, se è stato creato un campo Uso funzionale contenente valori di elenchi di selezione, è possibile impostare una condizione di filtro in cui Uso funzionale è uguale a *Vendite*.

6. Se lo si desidera, per evitare che i record contenuto occupino tutta la memoria di un dispositivo mobile, selezionare il secondo pulsante di opzione sotto Imposta limite massimo dei record e immettere il numero massimo di record contenuto che questa configurazione può trasferire ai dispositivi mobili. Utilizzare gli elenchi a discesa Ordina per e Ordina per specificare quali record vengono sincronizzati se viene superato il limite alle dimensioni dei dati per la configurazione mobile.
7. Fare clic su **Chiudi**.

VEDERE ANCHE:

Impostazione di Salesforce Classic mobile

## Configurazione dell'accesso a Salesforce Classic mobile per gli utenti partner

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le configurazioni, le serie di dati, i dispositivi mobili e gli utenti di Salesforce Classic mobile:

- "Visualizza impostazione e configurazione"

Per creare, modificare o eliminare configurazioni e serie di dati di Salesforce Classic mobile, provare configurazioni mobili, modificare proprietà di oggetti mobili e gestire le visualizzazioni personalizzate mobili:

- "Gestisci configurazioni mobili"

Nota: A partire dal rilascio Summer '13, il Portale partner non sarà più disponibile per le organizzazioni che non lo utilizzano già. Le organizzazioni esistenti potranno continuare ad accedervi regolarmente. Se non si dispone di un Portale partner ma si desidera condividere facilmente record e informazioni con i partner, provare a utilizzare le comunità.

Le organizzazioni esistenti che utilizzano Portali partner possono continuare a utilizzarli o passare a Communities. Per ulteriori informazioni, rivolgersi al responsabile account Salesforce.

È possibile consentire agli utenti partner l'accesso ai dati del Portale partner da dispositivo mobile mediante l'applicazione Salesforce Classic mobile.

Suggerimenti per impostare l'accesso a Salesforce Classic mobile per gli utenti partner:

- Prima di impostare Salesforce Classic mobile per gli utenti partner è necessario configurare gli account degli utenti partner e acquistare licenze mobili per ciascun utente del Portale partner che utilizzerà Salesforce Classic mobile. Affinché gli utenti partner possano utilizzare Salesforce Classic mobile è necessario che i profili degli utenti partner siano assegnati ad almeno un Portale partner attivo. Se un profilo utente viene assegnato a più Portali partner, solo il primo Portale partner assegnato sarà accessibile con Salesforce Classic mobile.
- Le visualizzazioni elenco mobili personalizzate non influiscono sulle visualizzazioni elenco del Portale partner.
- Se si rendono disponibili le serie di dati utente nell'applicazione Salesforce Classic mobile, i partner potranno assegnare oggetti ai loro utenti account partner e a tutti gli utenti interni. Se non si rendono disponibili le serie di dati utente, i partner potranno assegnare oggetti solo a utenti interni o a utenti account partner che siano associati a record resi disponibili sul dispositivo mobile.

VEDERE ANCHE:

Impostazione di Salesforce Classic mobile

## Creazione di link al Web e alle pagine Visualforce Mobile per Salesforce Classic mobile

Per migliorare l'integrazione tra l'applicazione Salesforce Classic mobile, Visualforce Mobile e i siti Web esterni, è possibile creare dei link tra record nativi di Salesforce e pagine Visualforce Mobile o siti Web esterni. Per creare i link, creare dei campi di testo formula su un oggetto standard o personalizzato. Per essere visualizzato in Salesforce Classic mobile, il campo deve essere visibile nel layout di pagina. È consigliabile includere tutti i link incorporati in una sezione separata denominata "Link mobili" nella parte inferiore del layout di pagina. Attualmente non vi è alcun modo di nascondere questi link in Salesforce, ma gli utenti possono ridurre a icona la sezione per togliere i link dalla pagina visualizzata.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per creare o modificare pulsanti o link personalizzati:
- "Personalizza applicazione"

1. Accedere all'area dei campi dell'oggetto appropriato.
2. Fare clic su **Nuovo** nella sezione Campi della pagina.
3. Selezionare `Formula` e fare clic su **Avanti**.
4. Immettere l'etichetta per il campo.

   Il nome del campo viene compilato automaticamente in base all'etichetta di campo immessa.
5. Selezionare `Testo` e fare clic su **Avanti**.
6. Nell'editor formule, creare il link alla pagina Visualforce personalizzata o al sito Web esterno:
   - Per creare un link a Visualforce, digitare *"visualforce:///apex/PageName"* sostituendo a *PageName* il nome della pagina Visualforce. Per passare le informazioni dal record dell'applicazione client alla pagina Visualforce è possibile aggiungere dei parametri in fondo alla stringa, ad esempio *?contactid=" & Id"*.
   - Per creare un link a un sito Web, digitare *"weblink:"* seguito dall'URL a cui dovrà puntare il link, ad esempio *"weblink:http://www.salesforce.com"*. Per passare le informazioni dal record dell'applicazione client alla pagina Web, è possibile aggiungere dei parametri in fondo alla stringa. Ad esempio, il link al sito Web riportato di seguito accede a un sito di social networking dal record di un referente ed esegue la ricerca del referente:

```
"weblink:http://m.linkedin.com/members?search_term=" &FirstName& "+" &LastName&
"&filter=name&commit=Search"
```

   Nota: l'applicazione client passa il link alla pagina Visualforce o alla pagina Web con tutti i parametri al browser incorporato. Gli eventuali parametri saranno interpretati dal sito Web o dalla pagina Visualforce Mobile. Avere cura di strutturare la pagina di Visualforce Mobile in modo che possa usufruire dei parametri passati nel link.

7. Fare clic su **Avanti**.
8. Impostare la protezione a livello di campo per determinare se il campo dovrà essere visibile o di sola lettura per profili specifici e fare clic su **Avanti**.
9. Scegliere i layout di pagina nei quali dovrà essere visualizzato il campo. Nella fase successiva si personalizzerà il layout per modificare la posizione del campo nella pagina.
10. Salvare le modifiche.
11. Modificare il layout di pagina dell'oggetto. Dalle impostazioni di gestione dell'oggetto per il quale si desidera modificare il layout di pagina, accedere a Layout di pagina.
12. Trascinare un elemento Sezione dalla tavolozza al layout di pagina e collocarlo sotto le sezioni esistenti.
13. Nel campo `Nome sezione`, digitare *Link mobili*.

14. Deselezionare l'opzione `Modifica pagina`.
15. Selezionare il layout a 1 colonna e fare clic su **OK**.
16. Trascinare il nuovo campo di testo formula dalla posizione attuale alla nuova sezione Link mobili.
17. Salvare le modifiche.

VEDERE ANCHE:

Impostazione di Salesforce Classic mobile

## Comunicare agli utenti la disponibilità di Salesforce Classic mobile

Quando si è pronti per distribuire l'applicazione Salesforce Classic mobile ai propri utenti, inviare loro un messaggio email per informarli della disponibilità dell'applicazione e fornire le istruzioni necessarie per l'installazione. È possibile inviare il messaggio email utilizzando l'applicazione email aziendale, ad esempio Outlook, oppure effettuare un invio globale da Salesforce. In entrambi i casi, includere l'URL che avvia il download.

- Per gli utenti di Android e BlackBerry, l'URL per il download è `mobile.salesforce.com`. Il link è lo stesso per il download iniziale e per gli aggiornamenti successivi.
- L'URL per il download per gli utenti di iPhone è disponibile su iTunes. Aprire iTunes, fare clic su **iTunes Store**, quindi cercare Salesforce Classic mobile. Per visualizzare informazioni sull'applicazione, fare clic sull'icona corrispondente. Nella parte superiore della finestra di iTunes è riportato un percorso che rappresenta la posizione dell'applicazione nell'App Store. **App Store** > **Business** > **Salesforce Classic mobile**. Trascinare e rilasciare il percorso in un editor di testo o in un programma di elaborazione testi per visualizzare l'URL per il download dell'applicazione.

Per inviare un messaggio email globale agli utenti di Salesforce Classic mobile da Salesforce:

1. Creare un modello di email che comunica agli utenti la disponibilità di Salesforce Classic mobile. Dalle impostazioni personali, immettere *`Modelli`* nella casella `Ricerca veloce` e selezionare **Modelli personali** o **Modelli di email**, a seconda della voce visualizzata. È anche possibile creare un secondo modello di messaggio per informare gli utenti che sono disponibili aggiornamenti. Includere nei modelli il link per il download.
2. Nella pagina Invio globale di email, creare una visualizzazione personalizzata che mostri solo gli utenti di Salesforce Classic mobile.

   Nota: la casella di controllo `Utente mobile` sul record utente assegna agli utenti una licenza mobile che consente di utilizzare la versione completa di Salesforce Classic mobile. Altri utenti di Salesforce possono tuttavia accedere alla versione gratuita di Salesforce Classic mobile senza che gli sia stata assegnata una licenza mobile; pertanto, non è possibile filtrare gli utenti in base alla licenza per visualizzare tutti gli utenti di Salesforce Classic mobile. È possibile invece creare una visualizzazione per gli utenti della versione gratuita filtrandoli in base ai ruoli o ai profili.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per creare modelli di email HTML:
- "Modifica modelli HTML"

Per eseguire un invio globale di email agli utenti:
- "Invio globale di email"

  E

  "Gestisci utenti"

3. Per inviare un messaggio email globale agli utenti di Salesforce Classic mobile, utilizzare la visualizzazione personalizzata che si è creata. Da Imposta, immettere *Utenti di email globali* nella casella Ricerca veloce, quindi selezionare **Utenti di email globali**.

VEDERE ANCHE:

Impostazione di Salesforce Classic mobile

## Domande frequenti su Salesforce Classic mobile per gli amministratori

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**



### L'app mobile Salesforce Classic mobile è sicura?

Tutti i dati trasmessi tra Salesforce e Salesforce Classic mobile sono completamente crittografati e protetti per la trasmissione over-the-air.

L'applicazione mobile dispone di più strati di protezione a livello del dispositivo. I fornitori di dispositivi mobili consentono di impostare limitazioni di accesso tramite password o codice di accesso. È necessario richiedere agli utenti di utilizzare la protezione dei dispositivi in base ai criteri di protezione dell'organizzazione. Se il dispositivo è bloccato da una password, è difficile per le persone non autorizzate appropriarsi di dati riservati.

Inoltre, un utente deve disporre di credenziali Salesforce valide per attivare l'applicazione mobile sul dispositivo. Quando un utente registra un nuovo dispositivo wireless, i dati Salesforce su tale dispositivo vengono cancellati automaticamente; gli utenti possono solo attivare un dispositivo mobile alla volta. Inoltre, gli utenti vengono avvisati quando un nuovo dispositivo viene attivato utilizzando il loro account Salesforce. Se un utente collegato supera il periodo di inattività configurato dall'amministratore sul dispositivo mobile, la sessione mobile viene interrotta e per ristabilirla è necessaria la password o il codice di accesso.

Gli amministratori possono anche eliminare i dati in remoto su qualsiasi dispositivo perso o rubato.

### Gli utenti di Salesforce Classic mobile utilizzano dispositivi Android, BlackBerry e iPhone. È possibile avere più tipi di dispositivi nella stessa organizzazione?

Sì, un'organizzazione può avere più tipi di dispositivi. Tuttavia, un utente di Salesforce Classic mobile può avere un solo dispositivo attivo.

### Esiste un modo semplice per distribuire Salesforce Classic mobile a tutti gli utenti BlackBerry?

Se l'organizzazione gestisce smartphone BlackBerry utilizzando il BlackBerry Enterprise Server (BES), è possibile utilizzare Application Push. Application Push è una tecnologia di erogazione avviata dagli amministratori sul BlackBerry Enterprise Server che installa applicazioni in remoto sugli smartphone BlackBerry. Questa tecnologia non è sviluppata né supportata da Salesforce, ma gli amministratori BlackBerry Enterprise Server possono utilizzarla per installare Salesforce Classic mobile sui dispositivi mobili BlackBerry dei loro utenti.

È possibile trovare informazioni dettagliate su Application Push nella *BlackBerry Enterprise Server Administrator Guide* ufficiale di Research in Motion, nelle sezioni "Making additional BlackBerry device software and applications available to users" e "Creating software configurations". In caso di problemi tecnici con Application Push, contattare l'assistenza di Research in Motion.

# Gestione delle configurazioni di Salesforce Classic mobile

Per gestire le configurazioni di Salesforce Classic mobile, da Imposta, immettere *Configurazioni Salesforce Classic* nella casella Ricerca veloce, quindi selezionare **Configurazioni Salesforce Classic**.

- Per definire una nuova configurazione mobile, fare clic su **Nuova configurazione mobile**.
- Per modificare una configurazione mobile, ad esempio per assegnare utenti o profili diversi e modificare le dimensioni massime delle serie di dati, fare clic su **Modifica**.
- Per attivare una configurazione mobile, fare clic su **Modifica**, selezionare la casella di controllo Attivo e fare clic su **Salva**. Per disattivare la configurazione mobile, deselezionare Attiva.
- Per eliminare una configurazione mobile, fare clic su **Canc**.
- Per visualizzare i dettagli di una configurazione mobile, fare clic sul nome corrispondente.

  Dalla pagina dei dettagli di una configurazione mobile è possibile:

  - Modificare le serie di dati di una configurazione mobile facendo clic su **Modifica** nell'elenco correlato Serie di dati.
  - Modificare le proprietà degli oggetti resi disponibili sui dispositivi mobili facendo clic su **Modifica** accanto al nome di un oggetto nell'elenco correlato Proprietà oggetto mobile.
  - Personalizzare le schede della configurazione mobile facendo clic su **Modifica** nell'elenco correlato Schede mobili.
  - Creare visualizzazioni personalizzate per una configurazione mobile facendo clic su **Modifica** nell'elenco correlato Visualizzazioni mobili.
  - Clonare la configurazione mobile facendo clic su **Clona**.

VEDERE ANCHE:

Panoramica su Salesforce Classic mobile per gli amministratori

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le configurazioni di Salesforce Classic mobile:

- "Visualizza impostazione e configurazione"

Per creare, modificare o eliminare configurazioni di Salesforce Classic mobile:

- "Gestisci configurazioni mobili"

## Gestione delle autorizzazioni di Salesforce Classic mobile

Ogni utente che accede alla versione completa del sito Salesforce Classic mobile deve disporre di una licenza mobile. Le licenze mobili si possono assegnare mediante la casella di controllo `Utente mobile` nel record dell'utente. Per le organizzazioni che utilizzano le versioni Unlimited Edition, Performance Edition e Developer Edition, Salesforce fornisce una licenza mobile per ogni licenza Salesforce e la casella di controllo `Utente mobile` è abilitata per impostazione predefinita per tutti gli utenti. Le organizzazioni che utilizzano la versione Professional Edition o Enterprise Edition devono invece acquistare le licenze a parte e assegnarle manualmente.

Nota: La casella di controllo `Utente mobile` è disabilitata per impostazione predefinita per i nuovi utenti della versione Performance Edition.

Per evitare che gli utenti attivino la versione completa di Salesforce Classic mobile sui loro dispositivi mobili prima che l'organizzazione sia pronta a implementare l'applicazione, disabilitare la casella di controllo `Utente mobile` per tutti gli utenti.

Gli utenti Salesforce che non dispongono di una licenza mobile possono scaricare una versione gratuita e limitata di Salesforce Classic mobile. A partire dal rilascio Spring '13, la versione gratuita di Salesforce Classic mobile è disabilitata per impostazione predefinita in tutte le nuove organizzazioni. È possibile abilitarla per consentire agli utenti di accedere a Salesforce sui loro dispositivi mobili.

Per abilitare la versione gratuita di Salesforce Classic mobile:

1. Da Imposta, digitare *`Impostazioni Salesforce Classic`* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni Salesforce Classic**.
2. Fare clic su **Modifica**.
3. Selezionare `Abilita Mobile Lite`.
4. Fare clic su **Salva**.

VEDERE ANCHE:

Panoramica su Salesforce Classic mobile per gli amministratori

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le configurazioni di Salesforce Classic mobile:

- "Visualizza impostazione e configurazione"

Per creare, modificare o eliminare configurazioni di Salesforce Classic mobile:

- "Gestisci configurazioni mobili"

## Gestione delle schede di Salesforce Classic mobile

Per gestire le schede di una configurazione Salesforce Classic mobile, da Imposta, immettere *Configurazioni Salesforce Classic* nella casella Ricerca veloce, quindi selezionare **Configurazioni Salesforce Classic**. Quindi, fare clic sul nome della configurazione mobile e scorrere verso il basso fino all'elenco correlato Schede mobili.

Se le schede della configurazione sono già state personalizzate, l'elenco correlato Schede mobili contiene le schede selezionate.

- Per modificare la configurazione di una scheda, fare clic su **Modifica**.
- Per eliminare l'impostazione della scheda mobile e utilizzare il comportamento predefinito della scheda, fare clic su **Ripristina predefinito**.

Se non è stata eseguita la personalizzazione delle schede della configurazione, l'elenco correlato indica che per la configurazione viene utilizzato il comportamento della scheda predefinita. Per personalizzare le schede utilizzate dalla configurazione e definirne l'ordine, fare clic su **Personalizza schede**.

VEDERE ANCHE:

Panoramica su Salesforce Classic mobile per gli amministratori

Gestione delle configurazioni di Salesforce Classic mobile

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le configurazioni di Salesforce Classic mobile:
- "Visualizza impostazione e configurazione"

Per gestire le schede di Salesforce Classic mobile:
- "Gestisci configurazioni mobili"

## Gestione delle visualizzazioni di Salesforce Classic mobile

Per gestire le visualizzazioni personalizzate di una configurazione Salesforce Classic mobile, da Imposta, immettere *Configurazioni Salesforce Classic* nella casella `Ricerca veloce`, quindi selezionare **Configurazioni Salesforce Classic**. Quindi, fare clic sul nome della configurazione mobile e scorrere verso il basso fino all'elenco correlato Visualizzazioni mobili.

- Per visualizzare l'elenco di tutte le proprie visualizzazioni personalizzate, scegliere Tutti gli oggetti dall'elenco a discesa `Selezionare un oggetto`. L'elenco a discesa Selezionare un oggetto può anche essere utilizzato per filtrare le visualizzazioni in base al tipo di oggetto.
- Per creare una nuova visualizzazione mobile, selezionare il tipo di oggetto dall'elenco a discesa Selezionare un oggetto, quindi fare clic su **Nuova visualizzazione mobile**.
- Per apportare delle modifiche a una visualizzazione mobile personalizzata, fare clic su **Modifica** accanto al nome della visualizzazione.
- Per eliminare una visualizzazione mobile personalizzata, fare clic su **Canc** accanto al nome della visualizzazione.
- Per visualizzare i dettagli relativi a una visualizzazione personalizzata mobile, fare clic sul suo nome.

VEDERE ANCHE:

Panoramica su Salesforce Classic mobile per gli amministratori
Gestione delle configurazioni di Salesforce Classic mobile
Gestione dei dispositivi di Salesforce Classic mobile

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare utenti e dispositivi di Salesforce Classic mobile:

- "Visualizza impostazione e configurazione"

Per gestire le visualizzazioni personalizzate di Salesforce Classic mobile:

- "Gestisci configurazioni mobili"

## Dati di utilizzo di Salesforce Classic mobile nei tipi di rapporto personalizzato

È possibile creare tipi di rapporto personalizzati contenenti dati che mostrano come l'organizzazione utilizza Salesforce Classic mobile. Ad esempio, i rapporti possono mostrare con quale frequenza gli utenti accedono a Salesforce Classic mobile, quali modelli di dispositivi mobili utilizzano, e così via.

Per creare un tipo di rapporto personalizzato con i dati di utilizzo di Salesforce Classic mobile, selezionare l'`Oggetto principale` della sessione mobile con dispositivo mobile durante la definizione di un tipo di rapporto personalizzato. Durante la selezione dei campi per il tipo di rapporto personalizzato, scegliere tra i seguenti campi specifici di Salesforce Classic mobile.

| Punto di dati utilizzo mobile | Definizione |
|---|---|
| Marca | Operatore wireless |
| Dimensioni dati (byte) | Dimensione totale dei record sul dispositivo |
| Indirizzo dispositivo | Indirizzo fisico univoco del dispositivo (PIN per BlackBerry o UDID per iOS) |
| Versione applicazione dispositivo | Versione installata di Salesforce Classic mobile |
| Modello dispositivo | Modello del dispositivo |
| Versione sistema operativo dispositivo | Versione del sistema operativo installato sul dispositivo |
| Durata | Durata della sessione mobile in secondi |
| Data ultima registrazione | Data dell'ultima registrazione o attivazione |
| Data ultimo stato | Data dell'ultima comunicazione ricevuta dal dispositivo |
| Produttore | Produttore del dispositivo |
| Dimensioni dei metadati (byte) | Dimensioni dei metadati (layout di pagina, valori di elenchi di selezione, ecc.) sul dispositivo |
| Titolare: Nome completo | Nome dell'utente del dispositivo |
| Data iniziale sessione | Data di inizio della sessione mobile |
| Stato | Indicatore che segnala che l'insieme di dati dell'utente supera le dimensioni massime consentite dalla configurazione mobile |

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per creare o aggiornare tipi di rapporto personalizzato:
- "Gestisci tipi di rapporto personalizzato"

Per eliminare i tipi di rapporto personalizzato:
- "Modifica tutti i dati"

Nota:

- Le sessioni mobili sono simili alle sessioni basate sul Web per quanto riguarda i rapporti sulla cronologia degli accessi; tuttavia, le sessioni mobili presentano un valore di timeout fisso di 20 minuti. Salesforce crea una nuova sessione mobile quando un utente accede a o avvia Salesforce Classic mobile dopo 20 minuti di inattività nell'applicazione o sul dispositivo in generale.
- I rapporti delle sessioni mobili presentano soltanto i dati di utilizzo per l'applicazione Salesforce Classic mobile e non per altre applicazioni mobili Salesforce come ad esempio quelle di Salesforce1.
- Alcuni dispositivi non forniscono tutti gli attributi fisici. Ad esempio, i dispositivi Apple non indicano la marca.

## Gestione dei dispositivi di Salesforce Classic mobile

Quando un utente installa l'applicazione Salesforce Classic mobile su un dispositivo mobile ed effettua il primo accesso, Salesforce raccoglie le informazioni sul dispositivo e lo associa al record dell'utente. Le informazioni relative al dispositivo sono di sola lettura.

Sebbene la voce del dispositivo venga creata automaticamente, è possibile continuare a visualizzare e gestire tutti gli utenti e i dispositivi mobili dell'organizzazione da Imposta immettendo *Utenti e dispositivi* nella casella `Ricerca veloce`, quindi selezionando **Utenti e dispositivi**.

Dalla pagina Tutti gli utenti e i dispositivi mobili è possibile:

- Visualizzare l'elenco degli utenti dell'organizzazione che sono stati abilitati all'utilizzo di Salesforce Classic mobile.
- Creare visualizzazioni elenco personalizzate per vedere i diversi sottoinsiemi di utenti mobili. Ad esempio, creare una visualizzazione che mostri gli utenti che non hanno mai eseguito l'accesso a Salesforce dall'applicazione Salesforce Classic mobile per valutare l'efficacia della distribuzione di Salesforce Classic mobile nella propria organizzazione.
- Visualizzare i dettagli di un dispositivo mobile facendo clic sull'indirizzo del dispositivo.
- Visualizzare i dettagli di un utente specifico, facendo clic sul nome utente corrispondente.
- Visualizzare i dettagli di una configurazione mobile, facendo clic sul nome corrispondente.
- Eseguire queste operazioni su più utenti contemporaneamente:
  - Regolare il valore di timeout della sessione mobile
  - Cancellare i dati di Salesforce dal dispositivo mobile di un utente
  - Eliminare un dispositivo mobile dal record di un utente
- Capire perché il dispositivo di un utente non esegue la sincronizzazione passando il mouse sull'icona di errore rossa nella colonna Stato. Nella pagina dei dettagli del dispositivo vengono visualizzate ulteriori informazioni sulla sincronizzazione.

Nota: è inoltre possibile gestire utenti mobili dall'elenco correlato Dispositivi mobili assegnati nella pagina dei dettagli degli utenti.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare utenti e dispositivi di Salesforce Classic mobile:
- "Visualizza impostazione e configurazione"

Per gestire i dispositivi di Salesforce Classic mobile:
- "Gestisci configurazioni mobili"

IN QUESTA SEZIONE:

Collegamento definitivo degli utenti Salesforce Classic mobile a un dispositivo mobile
È possibile impedire agli utenti mobili di registrare dispositivi mobili diversi da quello utilizzato per l'attivazione iniziale di Salesforce Classic mobile.

Visualizzazione delle informazioni sui dispositivi Salesforce Classic mobile

Impostazione dei valori di timeout per le sessioni di Salesforce Classic mobile

Cancellazione di dati in Salesforce Classic mobile

Eliminazione di dispositivi mobili

VEDERE ANCHE:

Panoramica su Salesforce Classic mobile per gli amministratori

Gestione delle configurazioni di Salesforce Classic mobile

## Collegamento definitivo degli utenti Salesforce Classic mobile a un dispositivo mobile

È possibile impedire agli utenti mobili di registrare dispositivi mobili diversi da quello utilizzato per l'attivazione iniziale di Salesforce Classic mobile.

Per impostazione predefinita, Salesforce associa automaticamente il record di un dispositivo all'ultimo utente mobile che lo ha attivato, quindi non è necessario che gli amministratori aggiornino il record del dispositivo per riassegnarlo a un altro utente. Sebbene questo comportamento consenta lo scambio semplice dei dispositivi tra gli utenti dell'organizzazione, alcuni amministratori preferiscono che gli utenti rimangano legati in modo definitivo ai dispositivi loro assegnati inizialmente. Ciò consente agli amministratori delle organizzazioni che possiedono dati altamente sensibili di assicurare che gli utenti non abbiano accesso ai dati aziendali dai loro dispositivi personali.

Per collegare in modo definitivo un utente a un dispositivo mobile:

1. Da Imposta, immettere *Impostazioni Salesforce Classic* nella casella Ricerca veloce, quindi selezionare **Impostazioni Salesforce Classic**.
2. Fare clic su **Modifica**.
3. Selezionare Collega in modo definitivo l'utente al dispositivo mobile.
4. Fare clic su **Salva**.

Avvertenza: L'abilitazione dell'impostazione Collega in modo definitivo l'utente al dispositivo mobile richiede un'azione di tipo amministrativo per consentire agli utenti di scambiarsi i dispositivi. Perché infatti l'utente possa registrare un dispositivo diverso, occorre infatti eliminare il dispositivo esistente manualmente dal record dell'utente. Se non si elimina il dispositivo, l'utente non sarà in grado di accedere all'applicazione Salesforce Classic mobile.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni di Salesforce Classic mobile:

- "Visualizza impostazione e configurazione"

Per modificare le impostazioni di Salesforce Classic mobile:

- "Gestisci configurazioni mobili"

## Visualizzazione delle informazioni sui dispositivi Salesforce Classic mobile

Quando un utente accede all'applicazione Salesforce Classic mobile per la prima volta, Salesforce raccoglie informazioni sul dispositivo dell'utente mobile. È possibile accedere ai dettagli dei dispositivi in due modi.

- Da Imposta, immettere *Utenti e dispositivi* nella casella `Ricerca veloce`, quindi selezionare **Utenti e dispositivi**. Fare clic sull'indirizzo di un dispositivo nella visualizzazione elenco.
- Da Imposta, immettere *Utenti* nella casella `Ricerca veloce`, quindi selezionare **Utenti**. Fare clic su **Modifica** accanto al nome di un utente, quindi fare clic sull'indirizzo del dispositivo nell'elenco correlato Dispositivi mobili assegnati.

Dalla pagina del dispositivo mobile, è possibile:

- Rivedere le informazioni sul dispositivo
- Regolare il valore di timeout della sessione mobile
- Cancellare i dati di Salesforce dal dispositivo di un utente
- Eliminare un dispositivo dal record di un utente

Di seguito è riportata una descrizione in ordine alfabetico dei campi memorizzati per ciascun dispositivo mobile dell'organizzazione.

| Campo | Descrizione |
| --- | --- |
| `Marca` | Marca del dispositivo mobile, se disponibile |
| `Operatore` | Nome dell'operatore che fornisce il servizio per il dispositivo mobile, se disponibile |
| `Connesso da` | Data e ora in cui il dispositivo mobile ha stabilito una connessione con il server mobile. Il dispositivo perde la connessione quando si esauriscono le batterie oppure quando la sessione viene chiusa perché il server non ha ricevuto dati dal dispositivo per un lungo periodo di tempo. |
| `Stato connessione` | Stato della connessione del dispositivo. I possibili valori di questo campo sono Connesso, Non connesso e Non disponibile. |
| `Creato da` | Nome del primo utente che ha registrato il dispositivo mobile e data e ora della registrazione |
| `Dimensioni dati` | Le dimensioni dei dati Salesforce attualmente archiviati nel dispositivo mobile dell'utente. Il dispositivo mobile invia periodicamente queste informazioni a Salesforce, una funzionalità che risulta utile per la risoluzione degli errori di sincronizzazione dovuti a un superamento del limite dei dati. |

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare utenti e dispositivi di Salesforce Classic mobile:
- "Visualizza impostazione e configurazione"

Per gestire i dispositivi di Salesforce Classic mobile:
- "Gestisci configurazioni mobili"

| Campo | Descrizione |
| --- | --- |
| Indirizzo dispositivo | Identificatore univoco del dispositivo mobile dell'utente |
| Modello dispositivo | Modello del dispositivo mobile |
| È simulatore? | Flag che indica se il dispositivo è un simulatore o un dispositivo mobile. Un simulatore è un'applicazione software che emula il comportamento di un dispositivo mobile. |
| Ultima attivazione | Data dell'ultimo download di un insieme completo di dati sul dispositivo mobile. Se i dati dell'utente superano il limite definito nella configurazione mobile assegnata, è possibile registrare il dispositivo, ma non attivarlo. |
| Ultimi dati ricevuti | Data dell'ultimo ricevimento di dati dal dispositivo. Questa informazione è utile per risolvere eventuali problemi di connessione. |
| Ultima registrazione | Data dell'ultima registrazione del dispositivo mobile da parte di un utente. Il processo di registrazione crea il record del dispositivo in Salesforce e lo associa all'utente che lo ha registrato. |
| Data ultimo stato | L'ultima volta che il dispositivo mobile ha notificato a Salesforce che non sta più eseguendo la sincronizzazione dei dati a causa di un errore. Il campo `Data ultimo stato` è visibile solo in presenza di un errore. |
| Produttore | Produttore del dispositivo mobile |
| Dimensioni metadati | Le dimensioni dei metadati di Salesforce attualmente archiviati nel dispositivo mobile dell'utente. I metadati sono informazioni relative ai layout di pagina e agli schemi; la quantità di metadati inviati a un dispositivo può essere molto grande in funzione delle dimensioni dell'organizzazione e della complessità della sua struttura. |
| Modificato da | Nome dell'ultimo utente che ha registrato il dispositivo mobile e data e ora della registrazione |
| Numero di messaggi in uscita in sospeso | Numero di messaggi in coda sul server mobile in attesa di essere inviati al dispositivo |
| Sistema operativo | Il tipo di sistema operativo installato sul dispositivo mobile: Android, BlackBerry o iPhone |
| Versione sistema operativo | Versione del sistema operativo installato sul dispositivo mobile. |
| Numero di telefono | Numero di telefono associato al dispositivo mobile |
| Versione Salesforce Classic mobile | Numero di versione e di build dell'applicazione client mobile installata sul dispositivo |
| Dimensioni messaggi in uscita in sospeso (byte) | Dimensioni totali dei dati dei messaggi in coda sul dispositivo in attesa di essere inviati al server mobile. Poiché il server elabora i |

| Campo | Descrizione |
|---|---|
| | messaggi quasi instantaneamente, questo valore è generalmente pari a 0. |
| `Dimensioni messaggi in uscita (byte)` | Dimensioni totali dei dati dei messaggi in uscita sul server mobile |
| `Stato` | Indica l'eventuale presenza di errori di sincronizzazione tra il dispositivo e Salesforce. Il campo `Stato` è visibile solo in presenza di un errore. I due stati di errore possibili sono Limite dimensione dei dati superato ed Errore sconosciuto. |
| `Nome utente` | Nome utente Salesforce dell'utente associato al dispositivo mobile |

Nota: se Salesforce rileva che il dispositivo selezionato è stato registrato da un utente di un'altra organizzazione, viene visualizzato un messaggio di errore nella pagina dei dettagli del dispositivo. Questa situazione può presentarsi quando un dispositivo è stato registrato a un utente nell'organizzazione sandbox e in seguito attivato da un utente nell'organizzazione di produzione. Per rimuovere il vecchio record del dispositivo dall'organizzazione, è sufficiente eliminare il dispositivo.

## Impostazione dei valori di timeout per le sessioni di Salesforce Classic mobile

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per impostare i valori di timeout delle sessioni di Salesforce Classic mobile:
- "Gestisci configurazioni mobili"

Per motivi di sicurezza, l'applicazione Salesforce Classic mobile è impostata in modo da bloccare gli utenti dopo 10 minuti di inattività. Gli amministratori possono regolare o disabilitare questa impostazione in base al dispositivo. Ad esempio, è possibile disabilitare l'impostazione del timeout di Salesforce Classic mobile se il sistema operativo del dispositivo mobile dispone di un proprio meccanismo di blocco.

Per modificare il valore di timeout delle sessioni di Salesforce Classic mobile:

1. Accedere a una di queste pagine:
   - Per gestire contemporaneamente più dispositivi, da Imposta, immettere *`Utenti e dispositivi`* nella casella `Ricerca veloce`, quindi selezionare **Utenti e dispositivi**. Nella visualizzazione elenco della pagina Utenti e dispositivi mobili, selezionare i dispositivi desiderati.
   - Per gestire un dispositivo specifico, da Imposta, immettere *`Utenti`* nella casella `Ricerca veloce`, quindi selezionare **Utenti**. Fare clic sul nome di un utente, quindi fare clic sull'indirizzo del dispositivo nell'elenco correlato Dispositivi mobili assegnati per visualizzare la pagina Dispositivo mobile.
2. Fare clic su **Imposta timeout sessione dispositivo mobile**.
3. Scegliere il nuovo valore di timeout in minuti. È anche possibile scegliere **Nessuna scadenza** per non bloccare l'accesso degli utenti all'applicazione.
4. Fare clic su **Salva**.

   Salesforce tenta di inviare un messaggio contenente la nuova impostazione del timeout di sessione ai dispositivi mobili selezionati.
5. Una pagina di conferma riassume i risultati di ogni dispositivo mobile selezionato.

### Risultati dell'impostazione dei valori di timeout per le sessioni con dispositivi mobili

Dopo che Salesforce ha inviato il nuovo valore di timeout ai dispositivi mobili selezionati, una pagina di risultati fornisce informazioni sullo stato di ciascun messaggio. Nella tabella riportata di seguito sono descritti i tre possibili risultati:

| Risultato | Descrizione |
| --- | --- |
| Messaggio accodato correttamente | Il server Salesforce Classic mobile ha inviato il messaggio al dispositivo. Salesforce non è in grado di rilevare se il messaggio è stato ricevuto dal dispositivo. |
| Impossibile inviare il messaggio | Un problema temporaneo di comunicazione tra Salesforce e il server Salesforce Classic mobile ha impedito l'invio del messaggio. Riprovare in seguito. |
| L'utente non ha un dispositivo mobile | L'utente mobile selezionato non ha mai registrato un dispositivo, pertanto non è stato possibile inviare il messaggio. |

## Cancellazione di dati in Salesforce Classic mobile

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per eliminare i dati di Salesforce su un dispositivo che esegue Salesforce Classic mobile:

- "Gestisci configurazioni mobili"

Quando un utente accede all'applicazione Salesforce Classic mobile, il suo dispositivo mobile contiene sia l'applicazione mobile che una serie di dati Salesforce dell'utente. L'amministratore può rimuovere i dati dal dispositivo senza disinstallare l'applicazione mobile. Questo garantisce un'efficace protezione quando un utente perde il proprio dispositivo. È inoltre necessario eliminare i dati da un dispositivo quando si prevede di consegnarlo a un altro utente.

Per cancellare i dati di Salesforce da uno o più dispositivi mobili:

1. Accedere a una di queste pagine:
   - Per gestire contemporaneamente più dispositivi, da Imposta, immettere *Utenti e dispositivi* nella casella `Ricerca veloce`, quindi selezionare **Utenti e dispositivi**. Nella visualizzazione elenco della pagina Utenti e dispositivi mobili, selezionare i dispositivi desiderati.
   - Per gestire un dispositivo specifico, da Imposta, immettere *Utenti* nella casella `Ricerca veloce`, quindi selezionare **Utenti**. Fare clic sul nome di un utente, quindi fare clic sull'indirizzo del dispositivo nell'elenco correlato Dispositivi mobili assegnati per visualizzare la pagina Dispositivo mobile.
2. Fare clic su **Cancella dati**, quindi su **OK**.

   Salesforce tenta di inviare un messaggio ai dispositivi mobili per cancellare i dati.

### Risultati della cancellazione dei dati

Dopo che Salesforce invia il messaggio ai dispositivi mobili per cancellare i dati, una pagina di risultati fornisce informazioni sullo stato di ciascun messaggio. Nella tabella riportata di seguito sono descritti i tre possibili risultati:

| Risultato | Descrizione |
| --- | --- |
| Messaggio accodato correttamente | Il server Salesforce Classic mobile ha inviato il messaggio al dispositivo. Salesforce non è in |

| Risultato | Descrizione |
|---|---|
| | grado di rilevare se il messaggio è stato ricevuto dal dispositivo. |
| Impossibile inviare il messaggio | Un problema temporaneo di comunicazione tra Salesforce e il server Salesforce Classic mobile ha impedito l'invio del messaggio. Riprovare in seguito. |
| L'utente non ha un dispositivo mobile | L'utente mobile selezionato non ha mai registrato un dispositivo, pertanto non è stato possibile inviare il messaggio. |

VEDERE ANCHE:

Gestione dei dispositivi di Salesforce Classic mobile

Eliminazione di dispositivi mobili

## Eliminazione di dispositivi mobili

I casi in cui si elimina un dispositivo mobile dal record di un utente possono essere due:

- Le impostazioni mobili dell'organizzazione collegano gli utenti mobili ai rispettivi dispositivi in modo permanente, ed è necessario assegnare un dispositivo a un utente diverso. Se non è stata abilitata questa impostazione, Salesforce associa automaticamente il record di un dispositivo all'ultimo utente mobile che lo ha attivato, quindi non è necessario eliminare un dispositivo per riassegnarlo a un altro utente.
- Si desidera spostare un dispositivo dall'organizzazione Sandbox all'organizzazione di produzione.

Per eliminare un dispositivo mobile:

1. Accedere a una di queste pagine:
   - Per gestire contemporaneamente più dispositivi, da Imposta, immettere *Utenti e dispositivi* nella casella `Ricerca veloce`, quindi selezionare **Utenti e dispositivi**. Nella visualizzazione elenco della pagina Utenti e dispositivi mobili, selezionare i dispositivi desiderati.
   - Per gestire un dispositivo specifico, da Imposta, immettere *Utenti* nella casella `Ricerca veloce`, quindi selezionare **Utenti**. Fare clic sul nome di un utente, quindi fare clic sull'indirizzo del dispositivo nell'elenco correlato Dispositivi mobili assegnati per visualizzare la pagina Dispositivo mobile.
2. Nella pagina Utenti e dispositivi mobili, selezionare uno o più dispositivi, quindi fare clic su **Elimina dispositivo**. Nella pagina Dispositivo mobile, fare clic su **Elimina**.
3. Fare clic su **OK**.

   Salesforce tenta di eliminare il dispositivo o i dispositivi selezionati.
4. Una pagina di conferma riassume i risultati di ogni dispositivo mobile selezionato.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Versione gratuita disponibile in: **tutte** le versioni tranne **Database.com** Edition

Versione completa disponibile nelle versioni: **Performance Edition**, **Unlimited Edition** e **Developer Edition** e, con un supplemento di prezzo, nelle versioni: **Professional Edition** ed **Enterprise Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare utenti e dispositivi mobili:
- "Visualizza impostazione e configurazione"

Per eliminare dispositivi mobili:
- "Gestisci configurazioni mobili"

### Eliminazione dei risultati dei dispositivi

Dopo che Salesforce ha inviato il messaggio al server mobile per eliminare i dispositivi, una pagina di risultati fornisce informazioni sullo stato di ciascun dispositivo. Nella tabella riportata di seguito sono descritti i tre possibili risultati:

| Risultato | Descrizione |
| --- | --- |
| Dispositivo eliminato. | Salesforce ha eliminato il record del dispositivo dall'organizzazione. |
| Impossibile eliminare il dispositivo in questo momento. Riprovare in seguito. | Un problema temporaneo di comunicazione tra Salesforce e il server mobile ha impedito l'eliminazione del dispositivo. Riprovare in seguito. |
| L'utente non ha un dispositivo mobile | L'utente mobile selezionato non ha mai registrato un dispositivo, pertanto non è stato possibile inviare il messaggio. |

VEDERE ANCHE:

Cancellazione di dati in Salesforce Classic mobile

# Chatter Mobile per BlackBerry

## Configurazione di Chatter Mobile per BlackBerry

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition**, **Contact Manager Edition**, **Developer Edition** e **Database.com Edition**

AUTORIZZAZIONI UTENTE

Per modificare le impostazioni delle applicazioni mobili:
- “Personalizza applicazione”

Per visualizzare le impostazioni delle applicazioni mobili:
- "Visualizza impostazione e configurazione"

**Importante:** A partire dal rilascio Summer '14, l'applicazione Chatter Mobile per BlackBerry non è più supportata. È possibile continuare a utilizzare l'applicazione, ma Salesforce non fornisce più l'assistenza sotto forma di correzioni di bug o ottimizzazioni per eventuali problemi che gli utenti dovessero riscontrare. Rivolgersi all'amministratore Salesforce per la migrazione all'app Salesforce1, la nuova esperienza mobile di Salesforce.

Chatter Mobile per BlackBerry funziona come un'applicazione connessa. Un'applicazione connessa è un'applicazione che si integra con Salesforce utilizzando le API. Le applicazioni connesse consentono agli amministratori di impostare diversi criteri di protezione e di avere un controllo esplicito su chi può utilizzare le applicazioni. Gli amministratori possono visualizzare e gestire le impostazioni di Chatter Mobile per BlackBerry nello stesso modo in cui visualizzano e gestiscono le impostazioni delle altre applicazioni connesse.

Chatter Mobile per BlackBerry viene installato automaticamente con un pacchetto di applicazioni connesse Salesforce gestite quando si verifica uno degli eventi che seguono:

- Un utente dell'organizzazione scarica l'applicazione mobile Chatter Mobile per BlackBerry e si autentica nell'organizzazione accedendo all'applicazione mobile.
- La sessione di un utente Chatter Mobile esistente si aggiorna.

  **Nota:** Le sessioni si aggiornano automaticamente tra ogni 15 minuti e 12 ore mentre un utente si trova nell'applicazione, in base all'impostazione `Valore timeout` della sessione impostato per l'organizzazione; spesso, questa attività non viene rilevata dall'utente.

In alternativa, un amministratore può installare manualmente il pacchetto di applicazioni connesse Salesforce1 e Chatter per visualizzare e gestire le impostazioni prima che il pacchetto venga installato automaticamente.

Il pacchetto di applicazioni connesse include un'applicazione connessa separata per il tipo di dispositivo mobile BlackBerry.

**Importante:** a meno che un amministratore non installi manualmente il pacchetto, l'applicazione connessa Chatter Mobile per BlackBerry sarà visualizzata solo dopo l'attivazione di un'applicazione mobile da parte di un utente dell'organizzazione o dopo l'aggiornamento della sessione di un utente esistente.

Per controllare l'accesso degli utenti all'applicazione, gli amministratori possono utilizzare i profili, gli insiemi di autorizzazioni e le restrizioni degli intervalli IP. Queste impostazioni vengono impostate pagina dei dettagli dell'applicazione connessa Chatter Mobile per BlackBerry, a cui si può accedere da Imposta immettendo *Applicazioni connesse* nella casella `Ricerca veloce`, quindi selezionando l'opzione per la gestione delle applicazioni connesse.

L'applicazione visualizza un messaggio di errore se un utente con accesso limitato tenta di aprirla.

# Mobile Dashboards for iPad

## Come consentire agli utenti di visualizzare i cruscotti digitali sull'iPad

L'app Mobile Dashboards for iPad è abilitata automaticamente per l'organizzazione, pertanto gli utenti possono accedervi senza necessità di alcuna configurazione.

**Importante:** a partire dal rilascio Summer '15, l'applicazione Mobile Dashboards for iPad non è più supportata. È possibile continuare a utilizzare l'applicazione, ma Salesforce non offre più il supporto sotto forma di correzione dei bug o miglioramenti per eventuali problematiche incontrate. Rivolgersi all'amministratore Salesforce per informazioni sulla migrazioni all'applicazione Salesforce1, la nuova esperienza mobile di Salesforce.

È possibile disattivare l'app se non si desidera che gli utenti accedano ai dati Salesforce dai dispositivi mobili e abilitarla nuovamente se in seguito si cambia idea.

Per configurare l'accesso a Mobile Dashboards for iPad:

1. Da Imposta, immettere *Cruscotti digitali mobili* nella casella `Ricerca veloce`, quindi selezionare **Impostazioni cruscotti digitali mobili**.
2. Selezionare o deselezionare `Abilita l'applicazione Mobile Dashboards for iPad per tutti gli utenti`.
3. Fare clic su **Salva**.

Gli utenti possono scaricare e installare l'app Mobile Dashboards for iPad dall'App Store di Apple o da AppExchange Mobile.

Oltre che per le versioni indicate sopra, l'applicazione è disponibile per le organizzazioni abilitate con l'API REST.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per visualizzare le impostazioni di Mobile Dashboards for iPad:

- "Visualizza impostazione e configurazione"

Per modificare le impostazioni di Mobile Dashboards for iPad:

- "Personalizza applicazione"

# Visualizzazione delle informazioni di registrazione push di un utente mobile

Dalla pagina Registrazioni push mobile, è possibile visualizzare le informazioni di registrazione push di qualsiasi utente per finalità generali di risoluzione dei problemi.

Per visualizzare le informazioni di registrazione push del dispositivo di un utente:

1. Da Imposta, immettere *Utenti* nella casella Ricerca veloce, quindi selezionare **Utenti**.
2. Selezionare un utente.
3. Nella pagina dei dettagli dell'utente, fare clic su Registrazioni push mobile, quindi su **Visualizza**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile in: Tutte le versioni

AUTORIZZAZIONI UTENTE

Per visualizzare le informazioni di registrazione push mobile:

- "Visualizza impostazione e configurazione"

# Installazione di pacchetti e gestione delle applicazioni

## Pacchetti installati

È possibile installare i pacchetti nell'organizzazione Salesforce, quindi configurarli e gestirli. Per visualizzare i pacchetti installati, da Imposta, immettere "Installato" nella casella Ricerca veloce e selezionare **Pacchetti installati**.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

# Installazione di un pacchetto

Di seguito è riportata la procedura di installazione di un pacchetto.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per installare i pacchetti:
- "Scarica pacchetti AppExchange"

## Fasi pre-installazione

1. In un browser, accedere all'URL di installazione fornito dallo sviluppatore del pacchetto oppure, se si sta installando un pacchetto da AppExchange, fare clic su **Scarica ora** nella pagina di informazioni sull'applicazione.

   Nota: Se si esegue l'installazione in un Sandbox, sostituire la porzione www.salesforce.com del link di installazione con test.salesforce.com. Il pacchetto viene rimosso dall'organizzazione Sandbox ogni volta che si crea una nuova copia del Sandbox.

2. Immettere il nome utente e la password per l'organizzazione Salesforce in cui si desidera installare il pacchetto e fare clic sul pulsante di accesso.
3. Se il pacchetto è protetto da password, immettere la password ricevuta dall'autore della pubblicazione.
4. Se necessario, se si sta installando un pacchetto non gestito, selezionare `Rinominare i componenti in conflitto nel pacchetto`. Quando si seleziona questa opzione, Salesforce modifica il nome di un componente nel pacchetto se tale nome è in conflitto con un nome di componente già esistente.

## Installazione predefinita

Fare clic su **Installa**. Verrà visualizzato un messaggio che descrive l'avanzamento e al termine dell'installazione apparirà un messaggio di conferma.

## Installazione personalizzata

Attenersi a questa procedura per modificare le impostazioni predefinite in qualità di amministratore.

1. Scegliere una o più delle seguenti opzioni, secondo le esigenze.
   - Fare clic su **Visualizza componenti**. Apparirà una sovrapposizione con un elenco dei componenti presenti nel pacchetto. Per i pacchetti gestiti, la schermata contiene anche un elenco di applicazioni connesse (applicazioni affidabili a cui è concesso l'accesso ai dati Salesforce di un utente una volta verificati sia l'utente che l'applicazione). Esaminare l'elenco per verificare che i componenti e tutte le applicazioni connesse siano accettabili, quindi chiudere la sovrapposizione.

     Nota: alcuni elementi del pacchetto, come le regole di convalida, i tipi di record e le impostazioni personalizzate, potrebbero non essere visualizzati nell'elenco dei componenti del pacchetto, ma vengono inclusi nel pacchetto e installati con gli altri elementi. Se nell'elenco dei componenti del pacchetto non sono presenti elementi, il pacchetto potrebbe contenere solo modifiche minime.

   - Se il pacchetto contiene un'impostazione di sito remoto, è necessario approvare l'accesso ai siti Web esterni a Salesforce. In questa finestra di dialogo sono elencati tutti i siti Web con i quali comunica il pacchetto. È consigliabile che il sito Web utilizzi SSL (Secure Sockets Layer) per la trasmissione dei dati. Dopo aver verificato la sicurezza dei siti Web, selezionare la casella **Sì, concedi l'accesso a questi siti Web esterni** e fare clic su **Continua** o su **Annulla** per annullare l'installazione del pacchetto.

     Avvertenza: Installando le impostazioni del sito remoto, si consente al pacchetto di trasmettere e ricevere dati da un sito Web di terze parti. Prima di utilizzare il pacchetto, contattare il publisher per individuare i dati trasmessi e la modalità

di utilizzo. Se è disponibile un referente interno per la sicurezza, richiedere l'analisi dell'applicazione e del suo impatto prima di utilizzarla.

- Fare clic su **Accesso API**. Viene visualizzata una sovrapposizione con un elenco delle impostazioni di accesso all'API che sono state concesse ai componenti del pacchetto. Esaminare le impostazioni per verificare che siano accettabili, quindi chiudere la sovrapposizione per tornare alla schermata di installazione.
- Nelle versioni Enterprise Edition, Performance Edition, Unlimited Edition e Developer Edition, scegliere una delle opzioni di protezione indicate di seguito.

Nota: a seconda del tipo di installazione, è possibile che questa opzione non sia visibile. Ad esempio, nelle versioni Group Edition e Professional Edition o se il pacchetto non contiene un oggetto personalizzato, Salesforce ignora questa opzione, concedendo accesso completo a tutti gli utenti.

**Installazione riservata agli amministratori**

Consente di specificare le impostazioni seguenti sul profilo dell'amministratore dell'installazione e sui profili con l'autorizzazione "Personalizza applicazione".

- Autorizzazioni sugli oggetti: “Lettura”, “Crea”, “Modifica”, “Elimina”, “Visualizza tutto” e “Modifica tutto” sono abilitate
- Protezione a livello di campo: impostata su visibile e modificabile per tutti i campi
- Classi Apex: abilitate
- Pagine Visualforce: abilitate
- Impostazioni dell'applicazione: abilitate
- Impostazioni delle schede: determinate dall'autore del pacchetto
- Impostazioni del layout di pagina: determinate dall'autore del pacchetto
- Impostazioni del tipo di record: determinate dall'autore del pacchetto

Dopo l'installazione, se si dispone della versione Enterprise Edition, Unlimited Edition, Performance Edition o Developer Edition, assegnare le autorizzazioni utente e oggetto appropriate ai profili personalizzati secondo le proprie necessità.

**Installazione per tutti gli utenti**

Consente di specificare le impostazioni seguenti su tutti i profili personalizzati interni.

- Autorizzazioni sugli oggetti: “Lettura”, “Crea”, “Modifica”, “Elimina”, “Visualizza tutto” e “Modifica tutto” sono abilitate
- Protezione a livello di campo: impostata su visibile e modificabile per tutti i campi
- Classi Apex: abilitate
- Pagine Visualforce: abilitate
- Impostazioni dell'applicazione: abilitate
- Impostazioni delle schede: determinate dall'autore del pacchetto
- Impostazioni del layout di pagina: determinate dall'autore del pacchetto
- Impostazioni del tipo di record: determinate dall'autore del pacchetto

Nota: I profili Utente Portale Clienti, Responsabile Portale Clienti, Utente Portale Clienti a volume elevato, Utente sito Web autenticato, Utente partner e i profili standard non ricevono alcun accesso.

**Installazione per profili specifici**

Consente di scegliere il livello di accesso per tutti i profili personalizzati dell'organizzazione. Ad ogni profilo può essere concesso l'accesso totale o nessun accesso per il nuovo pacchetto e tutti i relativi componenti.

- Accesso completo: consente di specificare le impostazioni che seguono per ogni profilo.
  - Autorizzazioni sugli oggetti: “Lettura”, “Crea”, “Modifica”, “Elimina”, “Visualizza tutto” e “Modifica tutto” sono abilitate
  - Protezione a livello di campo: impostata su visibile e modificabile per tutti i campi

- Classi Apex: abilitate
- Pagine Visualforce: abilitate
- Impostazioni dell'applicazione: abilitate
- Impostazioni delle schede: determinate dall'autore del pacchetto
- Impostazioni del layout di pagina: determinate dall'autore del pacchetto
- Impostazioni del tipo di record: determinate dall'autore del pacchetto

– Nessun accesso - Consente di specificare le stesse impostazioni di Accesso completo, *con la differenza che* tutte le autorizzazioni sugli oggetti sono disabilitate.

È possibile che siano visualizzate altre opzioni se l'autore della pubblicazione ha incluso impostazioni per profili personalizzati. Le impostazioni dei profili personalizzati dell'autore della pubblicazione possono essere incorporate nei propri profili senza alcun effetto sulle impostazioni. Scegliere il nome delle impostazioni del profilo dall'elenco a discesa accanto al profilo a cui si desidera applicarle. Le impostazioni correnti in tale profilo rimarranno inalterate.

In alternativa, fare clic su **Imposta tutto** accanto a un livello di accesso per assegnare questa impostazione a tutti i profili utente.

2. Fare clic su **Installa**. Verrà visualizzato un messaggio che descrive l'avanzamento e al termine dell'installazione apparirà un messaggio di conferma.
   - Durante l'installazione, Salesforce controlla e verifica le dipendenze. Perché l'installazione sia completata correttamente, è necessario che l'organizzazione di installazione soddisfi tutti i requisiti di dipendenza elencati nella pagina Mostra dipendenze. Ad esempio, per installare un pacchetto che fa riferimento alle divisioni è necessario che nell'organizzazione di installazione siano abilitate le divisioni.
   - Quando si installa un componente che contiene Apex, vengono eseguiti tutti i test di unità per l'organizzazione, compresi quelli contenuti nel nuovo pacchetto. Se un test di unità si basa su un componente inizialmente installato come inattivo, ad esempio una regola di flusso di lavoro, il test potrebbe non riuscire. È possibile selezionare l'installazione indipendentemente dall'esito del test.
   - Se l'installazione non riesce, vedere Perché la mia installazione o il mio aggiornamento non sono riusciti? a pagina 773.

## Fasi post-installazione

Se il pacchetto include istruzioni da seguire dopo l'installazione, verranno visualizzate al termine dell'installazione. Esaminare e seguire le istruzioni fornite. Inoltre, prima di distribuire il pacchetto agli utenti, apportare le modifiche necessarie alla propria implementazione. In base ai contenuti del pacchetto, potrebbe essere necessario effettuare alcune delle attività di personalizzazione descritte di seguito.

- Se il pacchetto include gli insiemi di autorizzazioni, assegnare gli insiemi di autorizzazioni inclusi agli utenti che ne hanno bisogno. Nei pacchetti gestiti, non è possibile modificare gli insiemi di autorizzazioni inclusi nel pacchetto, ma gli aggiornamenti successivi avvengono automaticamente. Se si clona un insieme di autorizzazioni fornito con un pacchetto gestito, oppure si crea il proprio insieme, sarà possibile modificare l'insieme di autorizzazioni, ma i successivi aggiornamenti non avranno alcun effetto.
- Se si sta reinstallando un pacchetto e si desidera importare nuovamente i dati del pacchetto mediante il file di esportazione ricevuto dopo la disinstallazione, vedere Importazione dei dati del pacchetto a pagina 765.
- Se è stato installato un pacchetto gestito, fare clic su **Gestisci licenze** per assegnare le licenze agli utenti.

  Nota: non è possibile assegnare licenze in Lightning Experience. Se è necessario assegnare una licenza, passare a Salesforce Classic.

- Configurare i componenti nel pacchetto secondo le proprie esigenze. Per ulteriori informazioni, vedere Configurazione dei pacchetti installati a pagina 756.

VEDERE ANCHE:

Aggiornamento dei pacchetti

Pacchetti installati

## Configurazione dei pacchetti installati

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per installare i pacchetti:
- "Scarica pacchetti AppExchange"

Per configurare i pacchetti installati:
- "Personalizza applicazione"

Molti componenti dispongono di un attributo **È distribuito** che stabilisce se sono disponibili per gli utenti finali. Dopo l'installazione, tutti i componenti sono immediatamente disponibili se erano disponibili nell'organizzazione dello sviluppatore. Prima di rendere il pacchetto disponibile agli utenti, apportare le modifiche necessarie alla propria implementazione. A seconda del contenuto del pacchetto, potrebbe essere necessario personalizzare i seguenti elementi:

**Opzione Configura**
Se l'autore pubblicazione ha incluso un link a un sito Web esterno con informazioni sulla configurazione, nella pagina dei download di AppExchange viene visualizzata un'opzione **Configura** accanto al pacchetto, in Imposta, quando si fa clic su **Pacchetti installati**. Fare clic su **Configura** per visualizzare le configurazioni consigliate dall'autore della pubblicazione.

**Campi e link personalizzati**
Aggiungere gli eventuali campi o link personalizzati necessari ai nuovi oggetti personalizzati.

**Oggetto personalizzato**
Abilitare il tracciamento per gli oggetti che non fanno parte di questo pacchetto ma che contengono campi di cui si tiene traccia in Chatter. Ad esempio, se si desidera tenere traccia di un campo personalizzato in Account, verificare che per l'oggetto standard Account sia stato abilitato il tracciamento.

**Tipi di rapporto personalizzato**
Se il `Nome tipo di rapporto` di un tipo di rapporto personalizzato corrisponde a un nome utilizzato nella propria organizzazione, cambiare il `Nome tipo di rapporto` dopo avere installato il pacchetto per evitare confusione tra i due tipi di rapporto.

**Utente in esecuzione per cruscotto digitale**
L'`Utente in esecuzione` dei cruscotti digitali è impostato sull'utente che installa il pacchetto. È possibile modificare le proprietà del cruscotto digitale e trasformare l'`Utente in esecuzione` in un utente che dispone delle impostazioni di protezione applicate al cruscotto digitale.

**Cartelle**
Quando le applicazioni contengono documenti, modelli di email, rapporti o cruscotti digitali, Salesforce crea nuove cartelle nell'organizzazione di installazione utilizzando i nomi delle cartelle dell'autore della pubblicazione. Accertarsi che questi nomi di cartelle siano univoci nella propria organizzazione.

Tutti gli utenti possono vedere le nuove cartelle. Configurare le impostazioni delle cartelle prima di distribuirle e utilizzarle se si desidera fare in modo che abbiano una visibilità limitata.

**Layout pagina iniziale**
I layout personalizzati per la pagina iniziale inclusi nel pacchetto non sono assegnati ad alcun utente. Per renderli disponibili agli utenti, assegnarli ai profili appropriati.

**Visualizzazioni elenco**

Le visualizzazioni elenco incluse nelle applicazioni sono visibili a tutti gli utenti. Se necessario, modificare la visibilità di queste visualizzazioni elenco.

**Layout di pagina**

A tutti gli utenti viene assegnato il layout di pagina predefinito per tutti gli oggetti personalizzati inclusi nel pacchetto. Gli amministratori di Enterprise Edition, Unlimited Edition, Performance Edition e Developer Edition possono configurare il layout di pagina per gli utenti appropriati.

Se un oggetto personalizzato del pacchetto include relazioni a oggetti standard, aggiungerle sotto forma di elenchi correlati nei relativi layout di pagina.

Se il pacchetto include link personalizzati, aggiungerli ai layout di pagina appropriati.

Se nell'organizzazione è attivata la gestione avanzata delle valute, i campi di riepilogo di roll-up valutari non sono validi se si trovano su valori di account e di opportunità di riepilogo oppure su valori di opportunità e di oggetti personalizzati di riepilogo. Eliminare tali campi da tutti i layout di pagina.

**Insiemi di autorizzazioni**

Assegnare gli insiemi di autorizzazioni inclusi in un pacchetto agli utenti che devono accedere al pacchetto.

Non è possibile modificare gli insiemi di autorizzazioni inclusi in un pacchetto gestito. Se si clona un insieme di autorizzazioni fornito con il pacchetto, oppure si crea il proprio insieme, sarà possibile modificare l'insieme di autorizzazioni, ma i successivi aggiornamenti non avranno alcun effetto.

**Area di lavoro traduzione**

I valori tradotti per i componenti dei pacchetti installati vengono installati anche per tutte le lingue che sono state incluse dallo sviluppatore. Tutti i componenti dei pacchetti personalizzati dallo sviluppatore all'interno della configurazione, ad esempio un tipo di campo o record personalizzato, vengono visualizzati nelle pagine di impostazione dell'autore dell'installazione nella lingua dello sviluppatore (cioè la lingua utilizzata al momento di definire tali componenti). Gli utenti dell'organizzazione di installazione visualizzano automaticamente i valori tradotti se la loro lingua è inclusa nel pacchetto. Inoltre, gli autori dell'installazione possono attivare delle lingue aggiuntive se l'Area di lavoro traduzione è abilitata.

**Avvisi di flusso di lavoro**

Se il destinatario di un avviso di flusso di lavoro è un utente, Salesforce sostituisce tale utente con quello che installa il pacchetto. È possibile modificare i destinatari di qualsiasi avviso di flusso di lavoro installato.

**Aggiornamenti di campo flusso di lavoro**

Se un aggiornamento di campo è progettato per sostituire il campo di un titolare di record con un utente specifico, Salesforce sostituisce tale utente con quello che installa il pacchetto. È possibile modificare il valore campo di qualsiasi aggiornamento di campo installato.

**Messaggi in uscita del flusso di lavoro**

Salesforce sostituisce l'utente nel campo `Invio da utente come` di un messaggio in uscita con quello che installa il pacchetto. È possibile modificare questo valore dopo l'installazione.

**Regole di flusso di lavoro**

Le regole di flusso di lavoro vengono installate senza alcun trigger basato su tempo eventualmente creato dallo sviluppatore. Impostare i trigger basati su tempo nel modo desiderato.

**Operazioni di flusso di lavoro**

Salesforce sostituisce l'utente nel campo `Assegnato a` con quello che installa il pacchetto. È possibile modificare questo valore dopo l'installazione.

Apportare tutte le altre modifiche eventualmente necessarie alla propria implementazione.

Nota: qualsiasi elemento aggiunto a un'applicazione personalizzata dopo l'installazione verrà rimosso assieme all'applicazione quando questa dovesse essere disinstallata.

VEDERE ANCHE:

Pacchetti installati

Considerazioni su Crittografia piattaforma

# Disinstallazione di un pacchetto

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per disinstallare i pacchetti:
- "Scarica pacchetti AppExchange"

È possibile rimuovere eventuali pacchetti installati, inclusi i relativi componenti e tutti i dati del pacchetto. Vengono inoltre rimossi eventuali campi personalizzati, link e qualsiasi altro elemento aggiunto all'applicazione personalizzata dopo l'installazione.

Per rimuovere un pacchetto:

1. Da Imposta, digitare *`Installato`* nella casella `Ricerca veloce` e quindi selezionare **Installato**.
2. Fare clic su **Disinstalla** accanto al pacchetto da rimuovere.
3. Selezionare `Sì, desidero disinstallare...` e fare clic su **Disinstalla**.
4. Dopo un'installazione, Salesforce crea automaticamente un file di esportazione che contiene i dati del pacchetto nonché tutti gli allegati e le note associati. Al termine della disinstallazione, Salesforce invia all'utente che l'ha eseguita un messaggio email contenente un link al file di esportazione. Il file di esportazione, gli allegati e le note associate sono riportati sotto l'elenco dei pacchetti installati. Si consiglia di archiviare il file in un altro percorso, poiché sarà disponibile per un periodo di tempo limitato dopo il completamente della disinstallazione.

   Suggerimento: se si reinstalla il pacchetto in seguito e si desidera reimportarne i dati, vedere Importazione dei dati del pacchetto a pagina 765.

## Note sulla disinstallazione di pacchetti

- Se si disinstalla un pacchetto che comprende un oggetto personalizzato, verranno eliminati anche tutti i relativi componenti, tra cui campi personalizzati, regole di convalida, S-Controls, pulsanti e link personalizzati, nonché regole di flusso di lavoro e processi di approvazione.
- Non è possibile disinstallare un pacchetto ogni volta che un componente che non sarà incluso nella procedura di disinstallazione fa riferimento a un componente del pacchetto. Ad esempio:
  - Quando un pacchetto installato comprende componenti di un oggetto standard cui fa riferimento un altro componente, Salesforce impedisce la disinstallazione del pacchetto. Questo significa che è possibile installare un pacchetto che comprenda un campo utente personalizzato e compilare una regola di flusso di lavoro che venga eseguita quando quel campo assume un dato valore. La disinstallazione del pacchetto impedirebbe l'esecuzione della regola di flusso lavoro.
  - Se sono installati due pacchetti non correlati contenenti ognuno un oggetto personalizzato e un componente dell'oggetto personalizzato fa riferimento a un componente contenuto nell'altro pacchetto, Salesforce impedisce la disinstallazione del pacchetto. Questo significa che è possibile installare un'applicazione di rapporti spese che comprenda un campo utente personalizzato e creare una regola di convalida per un altro oggetto personalizzato installato che faccia riferimento a quel campo utente personalizzato. Tuttavia, la disinstallazione dell'applicazione di rapporti spese impedisce l'esecuzione della regola di convalida.
  - Quando una cartella installata contiene componenti aggiunti dopo l'installazione, Salesforce impedisce di disinstallare il pacchetto.

- Quando una carta intestata installata viene utilizzata per un modello di email aggiunto dopo l'installazione, Salesforce impedisce di disinstallare il pacchetto.

- Non è possibile eliminare un pacchetto se un campo aggiunto al pacchetto viene aggiornato da un processo in background, ad esempio un aggiornamento a un campo di riepilogo di roll-up. Attendere il completamento del processo in background e riprovare.
- I file di esportazione di disinstallazione contengono dati dell'applicazione personalizzata per il pacchetto, tranne componenti quali documenti e valori di campi formula.

# Gestione delle installazioni dei pacchetti

Per visualizzare l'elenco dei pacchetti installati da AppExchange e i file di esportazione dei dati dei pacchetti disinstallati, fare clic su **Pacchetti installati**. Questi pacchetti possono essere gestiti o non gestiti.

Nota: Salesforce elenca soltanto le informazioni di licenza relative ai pacchetti gestiti. Nel caso dei pacchetti non gestiti, i campi correlati alla licenza, quali **Licenze consentite**, **Licenze utilizzate** e **Data scadenza**, contengono il valore "N/D".

Da questo elenco è possibile:

- Fare clic su **Disinstalla** per rimuovere il pacchetto e tutti i relativi componenti dall'organizzazione Salesforce.
- Fare clic su **Gestisci licenze** per assegnare le licenze disponibili agli utenti nell'organizzazione. Non è possibile assegnare licenze in Lightning Experience. Se è necessario assegnare una licenza, passare a Salesforce Classic.

  Nota: se è stata acquistata una licenza sito o se il pacchetto gestito non dispone di licenza, Salesforce assegna una licenza a tutti gli utenti e non è possibile gestire le licenze. Gli utenti possono utilizzare il pacchetto a condizione che dispongano delle autorizzazioni appropriate.

- Fare clic su **Configura** se l'autore della pubblicazione ha incluso un link a un sito Web esterno con informazioni sulla configurazione del pacchetto.
- Per visualizzare informazioni su un pacchetto, fare clic sul nome del pacchetto desiderato.
- Visualizzare l'autore della pubblicazione del pacchetto.
- Visualizzare lo stato delle licenze per questo pacchetto. I valori disponibili comprendono:
  - Prova
  - Attivo
  - Sospeso
  - Scaduto
  - Gratuito

  Il campo è visualizzato solo se il pacchetto è gestito e concesso in licenza.

- Tenere traccia del numero di licenze disponibili (`Licenze consentite`) e del numero di licenze assegnate agli utenti (`Licenze utilizzate`).
- Visualizzare la data di scadenza delle licenze relative a questo pacchetto.
- Visualizzare la data in cui le licenze sono state installate.
- Visualizzare il numero di applicazioni, schede e oggetti personalizzati contenuti in questo pacchetto.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per disinstallare i pacchetti:
- "Scarica pacchetti AppExchange"

Per assegnare le licenze per un pacchetto gestito:
- "Gestisci licenze pacchetto"

Per scaricare o eliminare il file di esportazione di un pacchetto disinstallato:
- "Scarica pacchetti AppExchange"

- Capire se le applicazioni, le schede e gli oggetti personalizzati vengono conteggiati nei limiti dell'organizzazione. In caso affermativo, la casella della colonna `Limiti` è selezionata.

> **Nota:** se non è stato installato un pacchetto gestito con licenza, i campi `Autore pubblicazione`, `Stato`, `Licenze consentite`, `Licenze utilizzate` e `Data scadenza` non sono visualizzati.

Dopo un'installazione, Salesforce crea automaticamente un file di esportazione che contiene i dati del pacchetto nonché tutti gli allegati e le note associati. Al termine della disinstallazione, Salesforce invia all'utente che l'ha eseguita un messaggio email contenente un link al file di esportazione. Il file di esportazione, gli allegati e le note associate sono riportati sotto l'elenco dei pacchetti installati. Si consiglia di archiviare il file in un altro percorso, poiché sarà disponibile per un periodo di tempo limitato dopo il completamente della disinstallazione. Da questo elenco è possibile:

- Fare clic su **Scarica** per aprire o archiviare il file di esportazione.
- Fare clic su **Canc** per eliminare il file di esportazione.

**Pacchetti gestiti e regole di condivisione scaduti**

Se una regola di condivisione basata su criteri fa riferimento a un campo di un pacchetto gestito la cui licenza è scaduta, dopo l'etichetta del campo viene aggiunta la dicitura `(scaduto)`. L'etichetta del campo è visualizzata nell'elenco a discesa dei campi nella pagina di definizione della regola in Imposta. Le regole di condivisione basate su criteri che fanno riferimento a campi scaduti non vengono ricalcolate e i nuovi record non vengono condivisi in base a queste regole. Viene invece conservata la condivisione dei record esistenti già prima della scadenza del pacchetto.

VEDERE ANCHE:

Visualizzazione dei dettagli di un pacchetto installato

Importazione dei dati dei pacchetti

# Visualizzazione dei dettagli di un pacchetto installato

La pagina dei dettagli di un pacchetto visualizza dettagli essenziali sul pacchetto installato da AppExchange. Per accedere alla pagina dei dettagli del pacchetto, da Imposta, immettere *Pacchetti installati* nella casella Ricerca veloce, selezionare **Pacchetti installati**, quindi fare clic sul nome del pacchetto che si desidera visualizzare.

Da questa pagina è possibile:

- Fare clic su **Disinstalla** per rimuovere il pacchetto e tutti i relativi componenti dall'organizzazione Salesforce.
- Fare clic su **Gestisci licenze** per assegnare le licenze disponibili agli utenti nell'organizzazione. Non è possibile assegnare licenze in Lightning Experience. Se è necessario assegnare una licenza, passare a Salesforce Classic.

  Nota: se è stata acquistata una licenza sito o se il pacchetto gestito non dispone di licenza, Salesforce assegna una licenza a tutti gli utenti e non è possibile gestire le licenze. Gli utenti possono utilizzare il pacchetto a condizione che dispongano delle autorizzazioni appropriate.

- Se lo si desidera, fare clic su **Visualizza dipendenze** e consultare l'elenco dei componenti che fanno affidamento su altri componenti, autorizzazioni o preferenze all'interno del pacchetto.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per disinstallare i pacchetti:
- "Scarica pacchetti AppExchange"

Per gestire le licenze utente per un pacchetto AppExchange:
- "Gestisci licenze pacchetto"

## Visualizzazione dei pacchetti installati

La pagina di un pacchetto installato visualizza i seguenti attributi del pacchetto (in ordine alfabetico):

| Attributo | Descrizione |
|---|---|
| Azione | Sono disponibili due opzioni:<br>• **Disinstalla**<br>• **Gestisci licenze** |
| Licenze consentite | Il numero complessivo delle licenze acquistate per questo pacchetto. Se si dispone di una licenza sito per questo pacchetto, il valore è "Illimitata". Il campo è visualizzato solo se il pacchetto è gestito e concesso in licenza. |
| Applicazioni | Il numero di applicazioni personalizzate nel pacchetto. |
| Applicazioni connesse | Un elenco delle applicazioni connesse che possono accedere ai dati Salesforce di un utente dopo la verifica sia dell'utente che dell'applicazione. |
| Descrizione | Una descrizione dettagliata del pacchetto. |
| Data di scadenza | La data di scadenza della licenza, in base ai termini e alle condizioni. Se il pacchetto non ha scadenza, la data di scadenza è "Nessuna |

| Attributo | Descrizione |
| --- | --- |
| | scadenza". Il campo è visualizzato solo se il pacchetto è gestito e concesso in licenza. |
| `Data installazione` | La data dell'installazione del pacchetto. |
| `Limiti` | Se selezionata, le applicazioni, le schede e gli oggetti personalizzati del pacchetto vengono conteggiati nei limiti dell'organizzazione. |
| `Spazio dei nomi` | L'identificativo alfanumerico di lunghezza compresa tra 1 e 15 caratteri che distingue il proprio pacchetto e il relativo contenuto da quelli di altri sviluppatori in AppExchange. |
| `Oggetti` | Il numero di oggetti personalizzati nel pacchetto. |
| `Nome pacchetto` | Il nome del pacchetto, assegnato dall'autore della pubblicazione. |
| `Autore della pubblicazione` | L'autore della pubblicazione di un elenco AppExchange è l'utente o l'organizzazione Salesforce che pubblica l'elenco. Il campo è visualizzato solo se il pacchetto è gestito e concesso in licenza. |
| `Stato` | Lo stato del pacchetto. I valori disponibili comprendono:<br>• Prova<br>• Attivo<br>• Sospeso<br>• Scaduto<br>• Gratuito<br>Il campo è visualizzato solo se il pacchetto è gestito e concesso in licenza. |
| `Schede` | Il numero di schede personalizzate nel pacchetto. |
| `Licenze utilizzate` | Il numero totale delle licenze già assegnate agli utenti. Il campo è visualizzato solo se il pacchetto è gestito e concesso in licenza. |
| `Nome versione` | Il nome della versione di questo pacchetto. Il nome della versione è il nome commerciale di un rilascio specifico di un pacchetto. È più descrittivo di `Versione`. |

## Visualizzazione dei dettagli di un pacchetto installato

La pagina dei dettagli di un pacchetto installato visualizza i seguenti attributi del pacchetto (in ordine alfabetico):

| Attributo | Descrizione |
| --- | --- |
| Accesso `API` | Il tipo di accesso all'API e ad Apex Code dinamico di cui dispongono i componenti del pacchetto. L'impostazione predefinita è **Senza restrizione**, il che significa che tutti i componenti del pacchetto che accedono all'API dispongono dello stesso livello di accesso dell'utente che ha effettuato l'accesso. Fare clic su **Abilita** |

| Attributo | Descrizione |
|---|---|
| | **restrizioni** o su **Disabilita restrizioni** per modificare le autorizzazioni di accesso API e Apex dinamico per un pacchetto. |
| `Applicazioni` | Il numero di applicazioni personalizzate nel pacchetto. |
| `Descrizione` | Una descrizione dettagliata del pacchetto. |
| `Numero prima versione installata` | La prima versione installata del pacchetto nell'organizzazione. Questo campo viene visualizzato soltanto per i pacchetti gestiti. È possibile fare riferimento a questa versione e ad altre versioni di pacchetto successive installate. Nel caso sia necessario riferire un problema con un pacchetto gestito all'autore della pubblicazione, inserire il numero di versione in questo campo. |
| `Installato da` | Il nome dell'utente che ha installato il pacchetto nell'organizzazione. |
| `Limiti` | Se selezionata, le applicazioni, le schede e gli oggetti personalizzati del pacchetto vengono conteggiati nei limiti dell'organizzazione. |
| `Modificato da` | Il nome dell'ultimo utente che ha modificato il pacchetto, comprese la data e l'ora. |
| `Spazio dei nomi` | L'identificativo alfanumerico di lunghezza compresa tra 1 e 15 caratteri che distingue il proprio pacchetto e il relativo contenuto da quelli di altri sviluppatori in AppExchange. |
| `Oggetti` | Il numero di oggetti personalizzati nel pacchetto. |
| `Nome pacchetto` | Il nome del pacchetto, assegnato dall'autore della pubblicazione. |
| `Tipo di pacchetto` | Indica se si tratta di un pacchetto gestito o non gestito. |
| `Istruzioni post-installazione` | Link alle informazioni relative alla configurazione del pacchetto dopo l'installazione. Come prassi consigliata, il link punta a un URL esterno; in questo modo è possibile aggiornare le informazioni indipendentemente dal pacchetto. |
| `Autore della pubblicazione` | L'autore della pubblicazione di un elenco AppExchange è l'utente o l'organizzazione Salesforce che pubblica l'elenco. Il campo è visualizzato solo se il pacchetto è gestito e concesso in licenza. |
| `Note di rilascio` | Link alle note di rilascio del pacchetto. Come prassi consigliata, il link dovrà puntare a un URL esterno, in modo che sia possibile rendere disponibili le informazioni prima del rilascio e aggiornarle indipendentemente dal pacchetto. |
| `Schede` | Il numero di schede personalizzate nel pacchetto. |
| `Nome versione` | Il nome della versione di questo pacchetto. Il nome della versione è il nome commerciale di un rilascio specifico di un pacchetto. È più descrittivo di `Versione`. |

| Attributo | Descrizione |
| --- | --- |
| `Versione` | Il numero dell'ultima versione del pacchetto installata. Il formato è *`majorNumber.minorNumber.patchNumber`*, ad esempio 2.1.3. Il numero di versione rappresenta il rilascio di un pacchetto. Il `Nome versione` è un nome più descrittivo del rilascio. `patchNumber` viene generato solo durante la creazione di una patch. Se non vi è alcun `patchNumber`, viene presunto che si tratti dello zero (0). |

## Componenti inutilizzati

È possibile vedere un elenco dei componenti eliminati dallo sviluppatore nella versione corrente del pacchetto. Se questo campo fa parte di un pacchetto gestito, non viene più utilizzato e può essere eliminato a meno che non sia stato utilizzato nelle integrazioni personalizzate. Prima di eliminare un campo personalizzato, per conservare un record dei dati da Imposta, digitare *`Esportazione dati`* nella casella `Ricerca veloce`, quindi selezionare **Esportazione dati**. Dopo che è stato eliminato, un componente inutilizzato compare in questo elenco per 15 giorni. Nel corso di questo periodo, è possibile annullare l'eliminazione per ripristinare il campo e tutti i dati in esso archiviati oppure eliminare il campo in modo permanente. Quando si annulla l'eliminazione di un campo, alcune delle sue proprietà vanno perse o vengono modificate. Dopo 15 giorni, il campo e i relativi dati vengono eliminati definitivamente.

Vengono visualizzate le seguenti informazioni sul componente (in ordine alfabetico):

| Attributo | Descrizione |
| --- | --- |
| `Azione` | Sono disponibili due opzioni:<br>• **Annulla Elimina**<br>• **Elimina** |
| `Nome` | Visualizza il nome del componente. |
| `Oggetto controllante` | Visualizza il nome dell'oggetto controllante a cui è associato un componente. Ad esempio, un oggetto personalizzato è controllante di un campo personalizzato. |
| `Tipo` | Visualizza il tipo di componente. |

## Componenti del pacchetto

È possibile visualizzare un elenco dei componenti inclusi nel pacchetto installato. Vengono visualizzate le seguenti informazioni sul componente (in ordine alfabetico):

| Attributo | Descrizione |
| --- | --- |
| `Azione` | Sono disponibili due opzioni:<br>• **Annulla Elimina**<br>• **Elimina** |
| `Nome` | Visualizza il nome del componente. |

| Attributo | Descrizione |
| --- | --- |
| `Oggetto controllante` | Visualizza il nome dell'oggetto controllante a cui è associato un componente. Ad esempio, un oggetto personalizzato è controllante di un campo personalizzato. |
| `Tipo` | Visualizza il tipo di componente. |

VEDERE ANCHE:

Importazione dei dati dei pacchetti

Gestione delle installazioni dei pacchetti

## Importazione dei dati dei pacchetti

Quando si disinstalla un pacchetto AppExchange, Salesforce crea automaticamente un file di esportazione che contiene i dati del pacchetto e tutte le note e gli allegati associati. Se si decide di installare nuovamente il pacchetto, è possibile importare questi dati.

Per importare i dati dei pacchetti AppExchange, utilizzare uno dei seguenti strumenti disponibili per la versione in uso:

- Per la versione Group Edition, utilizzare l'importazione guidata appropriata.
- Per la versione Professional Edition, utilizzare l'importazione guidata appropriata o qualunque strumento di integrazione di un partner ISV Salesforce compatibile.
- Per le versioni Enterprise Edition, Developer Edition, Performance Edition e Unlimited Edition, utilizzare Data Loader.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic e Lightning Experience

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per importare i dati dei pacchetti Force.com AppExchange:

- Le autorizzazioni richieste per utilizzare lo strumento di importazione prescelto, ad esempio l'importazione guidata o Data Loader.

### Note sull'importazione dei dati dei pacchetti AppExchange

- Durante l'esportazione, Salesforce converte i campi data in campi data/ora. Convertire i campi appropriati in campi data prima dell'importazione.
- Salesforce esporta tutti i campi data/ora nel fuso orario dell'Ora di Greenwich (GMT). Prima di importare questi campi, convertirli nel fuso orario appropriato.
- Il valore dei campi di numerazione automatica potrebbe essere diverso quando si esegue l'importazione. Per conservare i valori precedenti, creare un nuovo campo di numerazione automatica personalizzato su un oggetto personalizzato prima di importare i dati.
- Durante l'importazione Salesforce aggiorna i campi di sistema quali `Data creazione` e `Data ultima modifica`. Per conservare i valori precedenti per questi campi, contattare l'assistenza Salesforce.
- Le relazioni non vengono incluse nel file di esportazione. Ricreare le eventuali relazioni di ricerca o record principale-record dettaglio dopo aver importato i dati.
- Gli ID dei tipi di record vengono esportati, ma non il nome del tipo di record.
- La cronologia dei campi non viene esportata.

- Ricreare tutte le eventuali personalizzazioni effettuate sul pacchetto dopo l'installazione.

VEDERE ANCHE:

Visualizzazione dei dettagli di un pacchetto installato

Gestione delle installazioni dei pacchetti

# Gestione delle licenze per i pacchetti installati

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per gestire le licenze per un pacchetto AppExchange:
- "Gestisci licenze pacchetto"

Quando nell'organizzazione si installa un pacchetto gestito da AppExchange, si acquista dallo sviluppatore o dall'autore della pubblicazione del pacchetto un certo numero di licenze. È possibile assegnare ciascuna licenza a un utente dell'organizzazione. Se si assegnano tutte le licenze disponibili, ma si desidera assegnare licenze ad altri utenti, è possibile riassegnare una licenza o acquistarne altre. Per avere altre licenze, contattare l'autore della pubblicazione del pacchetto gestito.

Nota: se è stata acquistata una licenza sito o se il pacchetto gestito non dispone di licenza, Salesforce assegna una licenza a tutti gli utenti e non è possibile gestire le licenze. Gli utenti possono utilizzare il pacchetto a condizione che dispongano delle autorizzazioni appropriate.

1. Da Imposta, digitare *Pacchetti installati* nella casella `Ricerca veloce` e quindi selezionare **Pacchetti installati**.
2. Fare clic su **Gestisci licenze** accanto al pacchetto.

   Nota: per assegnare le licenze per un pacchetto, è necessario avere accesso al pacchetto e almeno una licenza disponibile.

   - Per assegnare le licenze a più utenti, fare clic su **Aggiungi utenti**.
   - Per rimuovere una licenza da un utente, fare clic su **Rimuovi** accanto al nome dell'utente. Per rimuovere le licenze da più utenti, fare clic su **Rimuovi più utenti**.
   - Fare clic sull'intestazione di una colonna per disporre gli utenti in ordine crescente in base ai dati della colonna stessa. Per disporre la colonna in ordine decrescente, fare nuovamente clic sull'intestazione.
   - Se disponibile, selezionare **meno** o **più** per ottenere un elenco di visualizzazione più breve o più lungo.

VEDERE ANCHE:

Assegnazione delle licenze per i pacchetti gestiti

Assegnazione delle licenze per i pacchetti installati

Rimozione delle licenze per i pacchetti installati

Risposta alle richieste di License Manager

# Assegnazione delle licenze per i pacchetti gestiti

Quando nell'organizzazione si installa un pacchetto gestito da AppExchange, si acquista dallo sviluppatore o dall'autore della pubblicazione del pacchetto un certo numero di licenze. È possibile assegnare ciascuna licenza a un utente dell'organizzazione. Se si assegnano tutte le licenze disponibili, ma si desidera assegnare licenze ad altri utenti, è possibile riassegnare una licenza o acquistarne altre. Per avere altre licenze, contattare l'autore della pubblicazione del pacchetto gestito.

L'elenco correlato Pacchetti gestiti nella pagina dei dettagli dell'utente riporta tutti i pacchetti gestiti assegnati all'utente. L'assegnazione di una licenza per un pacchetto gestito rende il pacchetto disponibile all'utente in Salesforce.

In questo elenco i pacchetti non gestiti non vengono visualizzati, dato che per essi non è possibile assegnare licenze.

Per assegnare a un utente una licenza per uno dei pacchetti gestiti disponibili:

1. Da Imposta, digitare *Utenti* nella casella `Ricerca veloce` e quindi selezionare **Utenti**.
2. Fare clic su **Assegna licenze** dall'elenco Pacchetti gestiti.
3. Selezionare il pacchetto da assegnare all'utente. Tutti i pacchetti gestiti disponibili sono riportati nell'elenco Pacchetti non assegnati. Una volta selezionato il pacchetto, Salesforce lo sposta automaticamente nell'elenco Pacchetti selezionati.

   L'elenco Pacchetti non assegnati visualizza tutti i pacchetti cui l'utente potrebbe accedere se gli fosse assegnata una licenza. Nell'elenco non compaiono i pacchetti non gestiti, non installati, già in uso o non disponibili.

   - Fare clic su una lettera per visualizzare i pacchetti i cui nomi iniziano con quella lettera o fare clic su **Tutti** per visualizzare tutti i pacchetti gestiti disponibili.
   - Fare clic su **selezionare mostrato** per selezionare tutti i pacchetti visualizzati nell'elenco Pacchetti non assegnati della pagina corrente, aggiungendoli all'elenco Pacchetti selezionati riportato di seguito.
   - Fare clic su **deselezionare mostrato** o **deselezionare tutto** per spostare i pacchetti dall'area Pacchetti selezionati all'area Pacchetti non assegnati.

4. Fare clic su **Aggiungi**.

Per revocare una licenza a un utente, fare clic su `Rimuovi` accanto al nome del pacchetto appropriato.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per modificare gli utenti:
- "Gestisci utenti interni"

Per gestire le licenze per un pacchetto AppExchange:
- "Gestisci licenze pacchetto"

VEDERE ANCHE:

Gestione delle licenze per i pacchetti installati

# Assegnazione delle licenze per i pacchetti installati

Per assegnare le licenze agli utenti Force.com AppExchange:

Nota: se è stata acquistata una licenza sito o se il pacchetto gestito non dispone di licenza, Salesforce assegna una licenza a tutti gli utenti e non è possibile gestire le licenze. Gli utenti possono utilizzare il pacchetto a condizione che dispongano delle autorizzazioni appropriate.

1. Da Imposta, immettere *Pacchetti installati* nella casella `Ricerca veloce`, quindi selezionare **Pacchetti installati** per trovare il pacchetto installato con licenze disponibili.
2. Fare clic sul link **Gestisci licenze** accanto al nome del pacchetto.
3. Fare clic su **Aggiungi utenti**.
4. Scegliere una visualizzazione dall'elenco a discesa oppure fare clic su **Crea nuova visualizzazione** per creare una nuova visualizzazione personalizzata.
5. Fare clic su una lettera per filtrare gli utenti il cui cognome corrisponde a quella lettera oppure fare clic su **Tutti** per visualizzare tutti gli utenti che soddisfano i criteri della visualizzazione corrente.
6. Selezionare gli utenti.
   - Per selezionare gli utenti singolarmente, utilizzare le caselle di controllo. Selezionare gli utenti riportati nell'elenco Selezionati. Quando l'elenco include tutti gli utenti ai quali si intende assegnare le licenze, fare clic su **Aggiungi**.
   - Per selezionare tutti gli utenti della visualizzazione corrente, fare clic su **Aggiungi tutti gli utenti**, quindi su **OK**.

Nota: è inoltre possibile aggiungere un solo utente dalla pagina dei dettagli dell'utente.

VEDERE ANCHE:

Gestione delle licenze per i pacchetti installati

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per gestire le licenze per un'applicazione AppExchange:

- "Gestisci licenze pacchetto"

# Rimozione delle licenze per i pacchetti installati

EDIZIONI

Disponibile in: Salesforce Classic

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per gestire le licenze per un pacchetto AppExchange:
- "Gestisci licenze pacchetto"

Per rimuovere le licenze per un pacchetto AppExchange da più utenti:

1. Da Imposta, digitare *Pacchetti installati* nella casella Ricerca veloce e quindi selezionare **Pacchetti installati**.
2. Fare clic su **Gestisci licenze** accanto al nome del pacchetto.
3. Fare clic su **Rimuovi più utenti**.
4. Per visualizzare un elenco di elementi filtrati, selezionare un elenco predeterminato dall'elenco a discesa Visualizza o fare clic su **Crea nuova visualizzazione** per definire le proprie visualizzazioni personalizzate.
5. Fare clic su una lettera per filtrare gli utenti il cui cognome corrisponde a quella lettera oppure fare clic su **Tutti** per visualizzare tutti gli utenti che soddisfano i criteri della visualizzazione corrente.
6. Selezionare gli utenti.
   - Per selezionare gli utenti singolarmente, utilizzare le caselle di controllo. Gli utenti selezionati vengono visualizzati nell'elenco Selezionato per la rimozione. Quando l'elenco include tutti gli utenti per i quali si desidera rimuovere le licenze, fare clic su **Rimuovi**.
   - Per selezionare tutti gli utenti della visualizzazione corrente, fare clic su **Rimuovi tutti gli utenti**, quindi su **OK**.

Per rimuovere le licenze per un pacchetto AppExchange da un solo utente, esistono diverse possibilità:

1. Da Imposta, digitare *Utenti* nella casella Ricerca veloce, quindi selezionare **Utenti** e fare clic su **Rimuovi** accanto al pacchetto nell'elenco dei pacchetti gestiti.
2. Da Imposta, digitare *Pacchetti installati* nella casella Ricerca veloce e quindi selezionare **Pacchetti installati**. Quindi, fare clic su **Gestisci licenze** accanto al nome del pacchetto e fare clic su **Rimuovi** accanto all'utente.

VEDERE ANCHE:

Gestione delle licenze per i pacchetti installati

## Risposta alle richieste di License Manager

Un'organizzazione License Manager è un'organizzazione Salesforce che tiene traccia di tutti gli abbonati Salesforce che installano un particolare pacchetto AppExchange. Gli amministratori di Salesforce possono scegliere di designare un'altra organizzazione come License Manager per uno dei loro pacchetti. L'organizzazione License Manager non deve necessariamente essere la stessa organizzazione che gestisce il pacchetto. Per scegliere un'altra organizzazione come License Manager, è sufficiente un indirizzo email (non un nome utente Salesforce). Se l'amministratore Salesforce sceglie di avere un'organizzazione License Manager di terze parti e inserisce l'indirizzo email dell'utente, l'utente riceverà una richiesta di gestione licenze.

Per rispondere a una richiesta di registrazione:

1. Fare clic sul link contenuto nel messaggio email di richiesta di gestione licenze. Verrà visualizzata la richiesta di registrazione nell'organizzazione Developer Edition di chi ha inviato la richiesta.
2. Fare clic su **Accetta** per completare il processo di registrazione. In alternativa, fare clic su **Rifiuta** per rifiutare la richiesta e chiudere il browser; in questo modo il link non sarà più utilizzabile.

   Nota: se si accetta la richiesta, si autorizza Salesforce a creare automaticamente dei record nella propria organizzazione Salesforce per tenere traccia dei dati relativi a questo pacchetto. La scelta di un'organizzazione come License Manager è definitiva e non può essere modificata.

3. Inserire il nome utente e la password dell'organizzazione Salesforce che si desidera utilizzare per gestire le licenze relative a questo pacchetto. Qualsiasi organizzazione Salesforce che abbia installato l'Applicazione License Management (LMA) gratuita da Force.com AppExchange può essere designata come organizzazione License Manager.
4. Fare clic su **Conferma**.

VEDERE ANCHE:

Gestione delle licenze per i pacchetti installati

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Developer Edition**

Le funzioni di caricamento e installazione di pacchetti sono disponibili nelle versioni **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per rispondere alle richieste di registrazione:
- "Personalizza applicazione"

## Assegnazione delle licenze utilizzando l'API

Gli amministratori possono utilizzare l'API per assegnare o revocare le licenze per qualsiasi pacchetto gestito installato nella loro organizzazione. Le informazioni di licenza relative a un pacchetto sono archiviate in due oggetti, PackageLicense e UserPackageLicense, a cui in precedenza si poteva accedere solo dalla pagina Gestisci licenze in Imposta. Questi sono ora accessibili come oggetti standard; pertanto, un amministratore può assegnare le licenze a utenti specifici mediante le chiamate API. Questo velocizza e semplifica la gestione delle licenze dei pacchetti in un'organizzazione abbonato, soprattutto per quanto riguarda le distribuzioni su vasta scala.

Ad esempio, si supponga che un amministratore installi un'applicazione che verrà utilizzata da tutti i 200 agenti di vendita della società. L'assegnazione di una licenza ad ogni agente di vendita dall'interfaccia utente sarebbe un processo lungo e poco efficiente. Utilizzando l'API, l'amministratore può assegnare le licenze a tutti gli agenti di vendita, in base ai loro profili, mediante un'unica operazione.

Segue un elenco di alcune operazioni comuni relative alle licenze che gli amministratori possono effettuare tramite l'API.

- Determinare il numero delle licenze pacchetto in uso e disponibili.
- Verificare se un determinato utente dispone della licenza per il pacchetto.
- Ottenere un elenco di tutti gli utenti che dispongono della licenza per il pacchetto.
- Assegnare una licenza pacchetto a un utente o a un gruppo di utenti.
- Revocare una licenza pacchetto precedentemente assegnata a un utente.

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per gestire le licenze per un'applicazione AppExchange:
- "Gestisci licenze pacchetto"

Per informazioni sugli oggetti PackageLicense e UserPackageLicense e un esempio di codice, vedere Riferimento oggetti per Salesforce e Force.com.

# Aggiornamento dei pacchetti

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**

AUTORIZZAZIONI UTENTE

Per caricare pacchetti:
- "Carica pacchetti AppExchange"

Per installare e disinstallare i pacchetti:
- "Scarica pacchetti AppExchange"

Salesforce supporta solo gli aggiornamenti dei pacchetti gestiti. Gli autori delle pubblicazioni possono pubblicare un aggiornamento per un pacchetto gestito e notificare gli autori dell'installazione che la nuova versione è disponibile. Gli autori dell'installazione di un pacchetto gestito possono quindi installare l'aggiornamento come segue.

1. Prima di installare un aggiornamento, verificare se l'applicazione installata faceva parte di un pacchetto gestito. Cercare l'icona Gestito - installato nella pagina dei dettagli di ciascun componente e nell'elenco dei pacchetti installati.

   Se l'applicazione installata non deriva da un pacchetto gestito, non sono disponibili aggiornamenti per quell'applicazione.

2. Quindi, installare l'aggiornamento seguendo la stessa procedura adottata per installare qualsiasi altro pacchetto contenuto in AppExchange. Se l'autore della pubblicazione ha fornito un link alla nuova versione, seguire il link per accedere al pacchetto e installarlo nell'organizzazione. Nella prima pagina della procedura guidata di installazione compaiono la versione attualmente installata, la versione che si sta per installare e un elenco dei componenti aggiuntivi compresi nella nuova versione.

## Note sull'aggiornamento di pacchetti gestiti

Quando si esegue l'aggiornamento di pacchetti gestiti, prestare attenzione ai seguenti punti:

- Tutti gli oggetti personalizzati esistenti precedentemente distribuiti saranno ancora distribuiti. Salesforce richiede di distribuire gli eventuali nuovi oggetti personalizzati o gli oggetti personalizzati che in precedenza non erano stati distribuiti.
- Le impostazioni dei profili per i componenti di un pacchetto possono essere modificate dal cliente ma non aggiornate dallo sviluppatore del pacchetto. Se lo sviluppatore apporta delle modifiche alle impostazioni dei profili dopo il rilascio del pacchetto, tali modifiche non verranno incluse in un aggiornamento. I clienti dovranno aggiornare manualmente le impostazioni dei profili dopo aver aggiornato il pacchetto. Gli insiemi di autorizzazioni invece possono essere aggiornati dallo sviluppatore, quindi le eventuali modifiche apportate dallo sviluppatore si rifletteranno nell'organizzazione del cliente dopo l'aggiornamento del pacchetto.
- Se lo sviluppatore sceglie di aggiungere campi personalizzati universalmente obbligatori, i campi avranno i valori predefiniti.
- I valori dell'area di lavoro traduzione per i componenti che sono "modificabili ma non aggiornabili" sono esclusi dagli aggiornamenti.
- Se un pacchetto installato dispone di accesso API `Con restrizione`, gli aggiornamenti saranno completati correttamente solo se la versione aggiornata non contiene S-Control. Se nella versione aggiornata sono presenti degli S-Control, è necessario cambiare l'accesso API del pacchetto installato in un accesso `Senza restrizione`.
- Quando si aggiorna un pacchetto, le modifiche all'accesso API vengono ignorate anche se è stato lo sviluppatore a specificarle. Ciò garantisce il controllo totale da parte dell'amministratore che installa l'aggiornamento. È opportuno che gli installatori esaminino con attenzione le modifiche all'accesso dei pacchetti durante l'installazione di ogni aggiornamento e prendano nota di tutte le modifiche accettabili. In seguito, poiché tali modifiche vengono ignorate, l'amministratore deve apportare manualmente tutte le modifiche accettabili dopo l'installazione di un aggiornamento.

# Domande frequenti sull'installazione di pacchetti

EDIZIONI

Disponibile nelle versioni: Salesforce Classic

Disponibile nelle versioni: **Group Edition**, **Professional Edition**, **Enterprise Edition**, **Performance Edition**, **Unlimited Edition** e **Developer Edition**



## È possibile disinstallare i pacchetti installati da AppExchange?

Sì. Tutti i pacchetti installati sono indicati nella pagina Pacchetti installati. È possibile rimuovere qualsiasi pacchetto facendo clic sul collegamento **Disinstalla** accanto al nome del pacchetto.

## Perché la mia disinstallazione non è riuscita?

Salesforce impedisce la disinstallazione di un pacchetto nei casi in cui questa operazione provochi il malfunzionamento dei componenti rimanenti.

## Chi può utilizzare AppExchange?

Chiunque può consultare gli elenchi di AppExchange ed effettuare prove. Gli amministratori e gli utenti di Salesforce dotati di autorizzazione "Scarica pacchetti AppExchange" possono installare le applicazioni AppExchange. Per pubblicare un'applicazione in AppExchange, gli utenti devono disporre sia dell'autorizzazione "Crea pacchetti AppExchange" che dell'autorizzazione "Carica pacchetti AppExchange".

## Perché la mia installazione o il mio aggiornamento non sono riusciti?

Un'installazione può avere esito negativo per diverse ragioni:

- Il pacchetto comprende oggetti personalizzati che determinerebbero il superamento del limite di oggetti personalizzati consentito per l'organizzazione.
- Il pacchetto comprende schede personalizzate che determinerebbero il superamento del limite di schede personalizzate consentito per l'organizzazione.
- Lo sviluppatore del pacchetto ha caricato una versione più recente del pacchetto e ha reso obsoleta la versione associata a questo URL di installazione. Contattare l'autore della pubblicazione del pacchetto per richiedere l'URL di installazione più recente.
- Si sta cercando di installare l'estensione di un pacchetto, senza che sia stato installato il pacchetto base.
- Il pacchetto richiede l'abilitazione di determinati componenti nell'organizzazione o di determinate funzionalità richieste nella versione in uso.
- Il pacchetto contiene Apex code e l'utente non è autorizzato a eseguire Apex nell'organizzazione.
- Il pacchetto che si sta installando non ha superato il test Apex.

## È possibile personalizzare i pacchetti di AppExchange?

Sì, tutti i pacchetti sono personalizzabili. Tuttavia, per garantire la compatibilità con le versioni future, alcuni aspetti dei pacchetti gestiti non si possono modificare.

Per un elenco dei componenti modificabili in un pacchetto gestito, vedere ISVforce Guide.

## Chi può utilizzare i pacchetti AppExchange?

Le organizzazioni che utilizzano le versioni Enterprise Edition, Unlimited Edition, Performance Edition o Developer Edition possono decidere quali profili utente potranno accedere al pacchetto durante il processo di installazione. Nelle organizzazioni con le versioni Professional Edition e Group Edition, i pacchetti vengono installati con "Accesso completo" per tutti i profili utente. Indipendentemente dalla versione, tuttavia, tutti gli oggetti personalizzati vengono installati in modalità "In fase di sviluppo", che li nasconde agli utenti standard. Per visualizzare gli oggetti personalizzati in modalità "In fase di sviluppo", è necessario che gli utenti dispongano dell'autorizzazione "Personalizza applicazione". Quando si sarà in procinto di distribuire il pacchetto ad altri utenti, modificare lo stato dell'oggetto personalizzato in "Utilizzato".

## Come posso aggiornare un pacchetto installato?

I pacchetti gestiti sono completamente aggiornabili. Prima di installare un pacchetto, contattare l'autore pubblicazione per determinare se il pacchetto è gestito.

## Qual è il livello di protezione dei componenti che si installano?

Salesforce effettua un riesame periodico della protezione di tutte le applicazioni presenti negli elenchi pubblici di AppExchange. Quando si installano applicazioni di terzi autorizzate ad accedere ai dati, tali applicazioni possono essere in grado di accedere ad altri dati all'interno dell'organizzazione in cui è stato installato il pacchetto. Gli elenchi privati non sono soggetti a controlli della protezione e pertanto gli amministratori devono esaminare attentamente l'applicazione prima di decidere se installarla o meno nelle rispettive organizzazioni.

## Che cosa succede al prefisso spazio dei nomi durante l'installazione di un pacchetto?

Il prefisso spazio dei nomi è un identificatore globalmente univoco che è possibile richiedere se si desidera creare un pacchetto gestito. Se si installa un pacchetto gestito che deriva da un altro sviluppatore, tutti i componenti di quel pacchetto contengono il prefisso spazio dei nomi assegnato nell'organizzazione a quello sviluppatore. Anche i pacchetti non gestiti possono avere un prefisso spazio dei nomi se derivano da un'organizzazione che conteneva un pacchetto gestito. Quando si installa un pacchetto non gestito che contiene un prefisso spazio dei nomi, Salesforce sostituisce il prefisso spazio dei nomi dello sviluppatore con quello dello sviluppatore che sta eseguendo l'installazione.

## È possibile reinstallare un pacchetto AppExchange dopo che è stato disinstallato?

Sì. La reinstallazione avviene secondo la stessa procedura utilizzata per la precedente installazione.

## Quando installo un pacchetto che è elencato in AppExchange, gli oggetti personalizzati, le schede e le app di quel pacchetto vengono conteggiati ai fini dei limiti della mia Salesforce Edition?

No. Se si installa un pacchetto da AppExchange, i relativi oggetti personalizzati, le schede e le app non vengono conteggiati ai fini dei limiti della Salesforce Edition in uso. Tuttavia, se il pacchetto utilizza altri tipi di componenti personalizzati, quali i campi personalizzati, questi vengono conteggiati nei rispettivi limiti della Salesforce Edition in uso.

**Nota:** Queste regole si applicano solo ai pacchetti gestiti elencati in AppExchange. Se si installa un pacchetto non gestito o un pacchetto gestito non elencato pubblicamente in AppExchange, i relativi oggetti personalizzati, le schede e le app vengono conteggiati ai fini dei limiti della Salesforce Edition in uso.

# INDICE ANALITICO

## B



## C

## D

## E

## S